This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

- Windows Operating Systems
  - Active Server Corner ASP Calendar Administrative Access
  - ASP-Rider Remote SQL Injection
  - **Code-Crafters Ability Server 'APPE FTP' Command Buffer Overflow (Updated)**
  - Computer Associates eTrust EZ Antivirus Local Insecure Default Installation
  - Crystal FTP Pro Buffer Overflow
  - **Digital Illusions Codename Eagle UDP Packet Processing Remote Denial of Service (Updated)**
  - Gadu-Gadu Multiple Remote Input Validation Vulnerabilities
  - Google Desktop Search
  - Interactive Studio GamePort Multiple Vulnerabilities
  - Kerio Technologies Multiple Kerio Products Universal Secret Key Storage
  - Microsoft Internet Explorer DHTML Edit Control Script Injection
  - **Microsoft IE Custom 404 Error Message & execCommand SaveAs File Download (Updated)**
  - Windows Media Player ActiveX Control Media File Attribute Corruption
  - **Microsoft WINS Name Validation (Updated)**
  - Novell NetMail Multiple Remote Vulnerabilities
  - Nullsoft Winamp Malformed MP4 Remote Denial of Service
  - **OpenText FirstClass HTTP Daemon Search Function Remote Denial of Service (Updated)**
  - RARLAB WinRAR File Name Remote Client-Side Buffer Overflow
  - VERITAS Backup Exec Buffer Overflow

UNIX / Linux Operating Systems

- Adobe Acrobat Reader mailListIsPdf() Buffer Overflow
- Amir Malik QwikMail Buffer Overflow
- Andrew W. Rogers pcal Buffer Overflows
- Anoakie Turner GREED 'DownloadLoop()' Function Vulnerabilities
- **Apple Safari Open Windows Injection (Updated)**
- Apple Safari Web Browser HTML Form Status Bar Misrepresentation
- **Atari800 Emulator Multiple Buffer Overflows (Updated)**
- atBas 2fax expandtabs() Buffer Overflow
- Bolthole Filter save_embedded_address() Buffer Overflow
- BSD csv2xml get_csv_token() Buffer Overflow
- BSD Junkie Input Validation Holes
- BSD tnftp mget() Input Validation Hole
- **Carsten Haitzler imlib Image Decoding Integer Overflow (Updated)**
- Chris Walshaw abc2mtex process_abc() Buffer Overflow
- Christoph Appel Perl Crypt::ECB Incorrect Block Encryption
- Christoph Dalitz abctab2ps Buffer Overflows
- **Cscope Insecure Temporary File Creation & #include Statement Buffer Overflow (Updated)**
- David Giffin xlreader book_format_sql() Buffer Overflow
- Gastón Kleiman Yanf get() Buffer Overflow
- **GD Graphics Library Remote Integer Overflow (Updated)**
- **GNU a2ps Filenames Shell Commands Execution (Updated)**
- GNU Aspell Stack Buffer Overflow
- GNU ChBg simplify_path() Buffer Overflow
- GNU Convex 3D readObjectChunk() Buffer Overflow
- GNU CUPS HPGL ParseCommand() Buffer Overflow
- GNU CUPS lppasswd Denial of Service
- GNU DXFscope dxfin() Buffer Overflow
- GNU jcabc2ps switch_voice() Buffer Overflow
- GNU jpegtoavi get_file_list_stdin() Buffer Overflow
- GNU MPlayer Processing ASF Streams Buffer Overflow
- GNU NapShare auto_filter_extern() Buffer Overflow
- GNU pgn2web process_moves() Buffer Overflow
- GNU rtf2latex2e ReadFontTbl() Buffer Overflow
- GNU unrtf process_font_table() Buffer Overflow
- GNU Vim / Gvim Modelines Command Execution Vulnerabilities
- GNU xine-lib Unspecified PNM and Real RTSP Clients Vulnerabilities
- GNU Yet Another MP3 Tool (YAMT) id3tag_sort() Input Validation Hole
- GPL Xine open_aiff_file() Buffer Overflow
- Guido Gonzato abcpp handle_directive() Buffer Overflow
- Helmut Cantzler Mesh Viewer dxfin() Buffer Overflow
- HP-UX newgrp Privilege Escalation

- html2hdml remove_quote() Buffer Overflow
- IBM AIX Multiple Privilege Escalation Vulnerabilities
- IglooFTP download_selection_recursive() Input Validation Hole
- **Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow (Updated)**
- J Whitham HTGET Buffer Overflow
- Jean-François Moine abcm2ps put_words() Buffer Overflow
- Jeff Dike uml_utilities umt_net slip_down() Denial of Service
- KDE Konqueror Java Sandbox Vulnerabilities
- **KDE Konqueror Window Injection (Updated)**
- **KDE Privacy Vulnerability (Updated)**
- Kerberos libkadm5srv Heap Overflow
- LGPL NASM error() Buffer Overflow
- **LibTIFF Buffer Overflows (Updated)**
- Little Igloo LinPopUp strexpand() Buffer Overflow
- Michael Hipp mpg123 find_next_file() Buffer Overflow
- Michael Kohn Ringtone Tools parse_emelody() Buffer Overflow
- Michael Kohn Visual Basic to C/GTK (vb2c) gettoken() Buffer Overflow
- Multiple Vendors ncpfs: ncplogin and ncpmap Buffer overflow
- **Multiple Vendors Emacs film Library Insecure Temporary File Creation (Updated)**
- **Multiple Vendors 'File' Processing ELF Headers Stack Overflow (Updated)**
- **Multiple Vendors glibc Buffer Overflow (Updated)**
- **Multiple Vendors Linux Kernel AF_UNIX Arbitrary Kernel Memory Modification (Updated)**
- Multiple Vendors Linux Kernel Auxiliary Message Layer State Error
- **Multiple Vendors Linux Kernel EXT3 File System Information Leakage (Updated)**
- **Multiple Vendors Linux Kernel Floating Point Register Contents Leak (Updated)**
- Multiple Vendors Linux Kernel IGMP Integer Underflow
- Multiple Vendors Linux Kernel ip_options_get() and vc_resize() Integer Overflows
- **Multiple Vendors Linux Kernel Local DoS & Memory Content Disclosure (Updated)**
- Multiple Vendors Linux Kernel Local DRM Denial of Service
- **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**
- Multiple Vendors Linux Kernel PROC Filesystem Local Information Disclosure
- **Multiple Vendors Linux Kernel ReiserFS File System Local Denial of Service (Updated)**
- Multiple Vendors Linux Kernel Sock_DGram_SendMsg Local Denial of Service
- **Multiple Vendors Linux Kernel 'sys32_ni_syscall' and 'sys32_vm86_warning' Buffer Overflows (Updated)**
- Multiple Vendors Linux Kernel Terminal Locking Race Condition
- Multiple Vendors Linux Kernel TIOCSETD Terminal Subsystem Race Condition
- **Multiple Vendors Linux Kernel USB Driver Kernel Memory (Updated)**
- **Multiple Vendors nfs-utils 'SIGPIPE' TCP Connection Termination Denial of Service (Updated)**
- Multiple Vendors Samba smbd Security Descriptor
- **Multiple Vendors Samba 'QFILEPATHINFO' Buffer Overflow (Updated)**
- **Multiple Vendors Samba Remote Wild Card Denial of Service (Updated)**
- **Multiple Vendors Linux Kernel BINFMT_ELF Loader Multiple Vulnerabilities (Updated)**
- **Multiple Vendors smbfs Filesystem Memory Errors Remote Denial of Service (Updated)**
- Namazu Cross-Site Scripting
- NetBSD compat Validation Flaws
- o3read parse_html() Buffer Overflow
- Open Source Technology Slash Unspecified Vulnerability
- OpenBSD isakmpd Error in pfkeyv2_acquire()
- Patric Müller Vilistextum get_attr() Buffer Overflow
- PHPGroupWare Multiple Cross-Site Scripting and SQL Injection
- PHPGroupware phpMyAdmin Two Vulnerabilities
- **PostgreSQL Insecure Temporary File Creation (Updated)**
- **Red Hat Information leak on Linux/ia64 (Updated)**
- Roxio Toast TDIXSupport Local Privilege Escalation
- **Russell Marks xzgv Integer Overflow (Updated)**
- **Russell Marks ZGV Image Viewer Multiple Remote Integer Overflow (Updated)**
- **Samba Remote Denials of Service (Updated)**
- Seymour Shlien abcMIDI dxfin() Buffer Overflow

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source

Active Server Corner ASP Calendar 1.0	A vulnerability exists which could let a remote malicious user obtain unauthorized administrative access. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Active Server Corner ASP Calendar Administrative Access	High	Bugtraq, December 14, 2004
ASP-Rider ASP-Rider	A vulnerability exists due the way user provided data is parsed, which could let a remote malicious user bypass the authentication mechanism and obtain administrative privileges. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ASP-Rider Remote SQL Injection	High	Securiteam, December 15, 2004
Code-Crafters Ability Server 2.25-2.34	A buffer overflow vulnerability exists in the processing of the APPE FTP command, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. **Exploit scripts have been published.**	Ability Server 'APPE FTP' Command Buffer Overflow	High	SecurityTracker Alert ID, 1012464, December 8, 2004 **SecurityFocus, December 16, 2004**
Computer Associates eTrust EZ Antivirus 7.0, 7.0.1 .1-7.0.1.4, 7.0.1, 7.0.2 .1, 7.0.2, 7.0.3, 7.0.4	A vulnerability exists due to insecure default file permissions on installed files, which could let a malicious user bypass security restrictions or obtain elevated privileges. Update available at: http://crm.my-etrust.com/login.asp?username=guest&target=DOCUMENT&openparameter=2222 There is no exploit code required.	Computer Associates eTrust EZ Antivirus Local Insecure Default Installation CVE Name: CAN-2004-1149	Medium	iDEFENSE Security Advisory, December 15, 2004
Crystal Art Software Crystal FTP Pro 2.8	A buffer overflow vulnerability exists due to a boundary error in the handling of file extensions in response to 'LIST' requests, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Crystal FTP Pro Buffer Overflow	High	Securiteam, December 19, 2004
Digital Illusions Codename Eagle 1.42 & prior	A remote Denial of Service vulnerability exists when a malicious user submits an empty UDP datagram. No workaround or patch available at time of publishing. **An exploit script has been published.**	Codename Eagle UDP Packet Processing Remote Denial of Service	Low	Secunia Advisory, SA13423, December 13, 2004 **SecurityFocus, December 13, 2004**
Gadu-Gadu Instant Messenger 6.0 build 149-build 155, 6.0	Multiple vulnerabilities exist: a vulnerability exists when parsing 'http:' and 'news:' links that are embedded in sent messages, which could let a remote malicious user execute arbitrary code; a vulnerability exists when a remote malicious user submits packets with embedded '.dll' files, which could let the client execute some of the functions; a vulnerability exists in the DCC connection feature, which could let a remote malicious user obtain sensitive information; a buffer overflow vulnerability exists due to a boundary error when sending images, which could let a remote malicious user execute arbitrary code; a vulnerability exists when small images are allowed to be sent even when the 'image send' option is disabled; a buffer overflow vulnerability exists when assembling divided sent files that contain specially crafted length values, which could let a remote malicious user execute arbitrary code; and an integer overflow vulnerability exists when handling receiving files through DCC that contain a specially crafted file length value. Users are advised to contact the vendor for more information on obtaining the fixed packages. There is no exploit script required; however, a Proof of Concept exploit has been published.	Gadu-Gadu Multiple Remote Input Validation Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA13450, December 17, 2004
Google Google Desktop Search prior to 121004	A vulnerability exists because it is possible for Java applets (and possibly JavaScript and other plug-ins) to trigger fake Google searches that will cause Google Desktop Search to return local results, which normally would be embedded in search results from Google. The vendor has released a fixed version (121004) as of December 10, 2004. Currently we are not aware of any exploits for this vulnerability. Vulnerability has appeared in the Press and other public media.	Google Desktop Search	Medium	Secunia Advisory, SA13567, December 21, 2004
Interactive Studio GamePort 3.0, 3.1, 4.0	Multiple vulnerabilities exist in the client and server that could let a remote malicious user obtain unauthorized access and execute arbitrary code. No workaround or patch available at time of publishing. An exploit has been published.	Interactive Studio GamePort Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bugtraq, December 17, 2004

Kerio Technologies Mailserver 5.0, 5.1, 5.1.1, 5.6.3-5.6.5, 5.7.0-5.7.10, 6.0-6.0.4, ServerFirewall 1.0, WinRoute Firewall 5.0.1-5.0.9, 5.1-5.1.10, 5.10, 6.0-6.0.8	A vulnerability exists because a universal secret key is used to extract plain text from credential hashes and is stored in the WinRoute Firewall, Kerio ServerFirewall, and Kerio MailServer binaries, which could let a malicious user obtain sensitive information. Updates available at: http://www.kerio.com/kwf_download.html http://www.kerio.com/ksf_download.html http://www.kerio.com/kms_download.html Currently we are not aware of any exploits for this vulnerability.	Multiple Kerio Products Universal Secret Key Storage CVE Name: CAN-2004-1022	Medium	The Secure Computer Group at the University of a Coruna & dotpi.com Information Technologies Research Labs Security Advisory, December 14, 2004
Microsoft Internet Explorer 6.0, SP1&SP2	A vulnerability exists in the DHTML Edit ActiveX control, which could let a remote malicious user inject arbitrary scripting code into a different window on the target user's system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer DHTML Edit Control Script Injection	High	Bugtraq, December 15, 2004
Microsoft Internet Explorer (IE) 6 on Windows XP SP2 and Windows 2000	A vulnerability exists that could permit a remote malicious user to invoke the execCommand 'SaveAs' function via a custom HTTP 404 Not Found error message to download arbitrary files to the target user's system without the XP SP2 warning messages. Internet Explorer does not properly process URLs with certain extraneous characters. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Microsoft IE Custom 404 Error Message & execCommand SaveAs File Download	High	SecuriTeam, November 22, 2004 **US-CERT Vulnerability Note, VU#743974, December 17, 2004**
Microsoft Windows Media Player 9.0	Two vulnerabilities exist: a vulnerability exists because the artist, album name, and song name information can be overwritten in a media file, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'getItemInfoByAtom()' function, which could let a remote malicious user obtain sensitive information. Update available at: http://www.microsoft.com/downloads/details.aspx?FamilyID=b446ae53-3759-40cf-80d5-cde4bbe07999&displaylang=en An exploit has been published.	Windows Media Player ActiveX Control Media File Attribute Corruption	Medium/ High	SecurityTracker Alert ID, 1012626, December 20, 2004
Microsoft Windows NT Server 4.0 SP 6a, NT Server 4.0 Terminal Server Edition SP 6, Windows 2000 Server SP 3 & SP4, Windows Server 2003, 2003 64-Bit Edition	A vulnerability exists due to an unchecked buffer in the handling of the 'Name' parameter from certain packets, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-045.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft WINS Name Validation CVE Name: CAN-2004-0567	High	Microsoft Security Bulletin, SB04-045, December 14, 2004 **US-CERT Vulnerability Note, VU#378160, December 16, 2004**
Novell NetMail 3.10, 3.10 a-3.10 g	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the IMAP functionality, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to a failure to properly integrate with Symantec antivirus software, which could let a remote malicious user bypass anti-virus screening; and several remote Denial of Service vulnerabilities exist. Updates available at: http://support.novell.com/servlet/filedownload/sec/pub/netmail310h.exe Currently we are not aware of any exploits for these vulnerabilities.	Novell NetMail Multiple Remote Vulnerabilities	Low/ Medium/ High (High if arbitrary code can be executed)	Novell Technical Information Document, TID2970425, December 13, 2004
NullSoft Winamp 5.07	A remote Denial of Service vulnerability exists due to a failure to properly process '.mp4' and '.m4a' files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Nullsoft Winamp Malformed MP4 Remote Denial of Service	Low	SecurityTracker Alert ID, 1012525, December 15, 2004
Open Text Corporation FirstClass 8.0	A remote Denial of Service vulnerability exists in the HTTP Daemon Search function. **Customers are advised to contact the vendor for further details in regard to obtaining and applying an appropriate fix.** **An exploit script has been published.**	OpenText FirstClass HTTP Daemon Search Function Remote Denial of Service	Low	SecurityTracker Alert ID, 1012478, December 11, 2004 **SecurityFocus, December 16, 2004**
RARLAB WinRar 3.0 .0, 3.0, 3.10, beta 5, beta 3, 3.11,	A client-side buffer overflow vulnerability exists in the file name functionality due to insufficient validation of user-supplied strings length prior to copying them into static process buffers, which could let a remote malicious user execute arbitrary code.	RARLAB WinRAR File Name Remote Client-Side Buffer Overflow	High	K-Otik Security Advisory, December 17, 2004

3.20, 3.40, 3.41	No workaround or patch available at time of publishing. An exploit script has been published.			
Veritas Software Backup Exec 8.0, 8.5, 8.6, 9.0, 9.1	A buffer overflow vulnerability exists due to a boundary error in the Agent Browser service when processing received registration requests, which could let a remote malicious user execute arbitrary code. Hotfix available at: http://seer.support.veritas.com/docs/273422.htm Currently we are not aware of any exploits for this vulnerability.	VERITAS Backup Exec Buffer Overflow CVE Name: CAN-2004-1172	High	Veritas Software Security Advisory, 273419, December 16, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Adobe Adobe Acrobat Reader 5.0.9 for Unix	A buffer overflow vulnerability exists in in Adobe Acrobat Reader for Unix. A remote malicious user can execute arbitrary code on the target system. A remote user can create a specially crafted PDF file that, when processed by the target user, will trigger a buffer overflow in the mailListIsPdf() function and execute arbitrary code. The code will run with the privileges of the target user. The vendor has issued a fixed version (5.0.10): http://www.adobe.com/support/techdocs/331153.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-12.xml Currently we are not aware of any exploits for this vulnerability.	Adobe Acrobat Reader mailListIsPdf() Buffer Overflow CVE Name: CAN-2004-1152	High	iDEFENSE Security Advisory 12.14.04 Gentoo Security Advisory, GLSA 200412-12 / acroread, December 16, 2004
Amir Malik QwikMail 0.3	A vulnerability was reported in QwikMail. A remote malicious user can send mail via the target system. A remote user can connect to the target service and send an SMTP string to enable the mail to be forwarded. The command will overflow a buffer allocated to hold the local IP address. The software permits the localhost (127.0.0.1) to relay mail. A fix is available via CVS at: http:http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/qwikmail/qwik-smtpd/ A Proof of Concept exploit has been published.	Amir Malik QwikMail Buffer Overflow	High	SecurityTracker Alert ID, 1012561, December 16, 2004
Andrew W. Rogers pcal 0.7.1	Two vulnerabilities were reported in pcal. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted calendar file that, when processed by the target user with pcal, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflows reside in the getline() function in 'pcalutil.c' and the get_holiday() function in 'readfile.c'. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Andrew W. Rogers pcal Buffer Overflows	High	SecurityTracker Alert ID, 1012592, December 16, 2004
Anoakie Turner GREED (Get and Resume Elite EDition) 0.81p	Multiple vulnerabilities exist in GREED, which can be exploited by malicious people to compromise a user's system. A boundary error and an input validation error in the 'DownloadLoop()' function can be exploited to cause a buffer overflow. No workaround or patch available at time of publishing. Proofs of Concept exploit scripts have been published.	Anoakie Turner GREED 'DownloadLoop()' Function	High	Secunia Advisory ID, SA13534, December 17, 2004
Apple Safari 1.2.4	A vulnerability exists which could allow a remote malicious user to inject content into an open window in certain cases to spoof web site contents. If the target name of an open window is known, a remote user can create Javascript that, when loaded by the target user, will display arbitrary content in the opened window. A remote user can exploit this to spoof the content of potentially trusted web sites. **Apple has issued a fix as part of Security Update 2004-12-02, available at:** **http://www.apple.com/swupdates/** A Proof of Concept exploit has been published.	Apple Safari Open Windows Injection	High	SecurityTracker Alert ID, 1012459, **December 10, 2004**
Apple Safari 1.0 - 1.2.3	A vulnerability exists that that allows a malicious user to misrepresent the status bar in the browser, allowing vulnerable users to be mislead into following a link to a malicious site. The issue presents itself when an user creates an HTML form with the submit 'value' property set to a legitimate site and the 'action' property set to the attacker-specified site. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Apple Safari Web Browser HTML Form Status Bar Misrepresentation	Medium	SecurityFocus Bugtraq ID,11949, December 15, 2004

Atari Atari800 1.3.1 & prior	Several buffer overflow vulnerabilities exist in the 'log.c' and 'rt-config.c' files due to insufficient boundary checks, which could let a malicious user execute arbitrary code with root privileges. The vendor reports that the vulnerability described in 'log.c' is fixed in versions after 2003-11-13, and that they are currently looking into the issue in 'rt-config.c'. **Debian:** **http://www.debian.org/security/2004/dsa-609** An exploit script has been published.	Atari800 Emulator Multiple Buffer Overflows CVE Name: CAN-2004-1076	High	Securiteam, November 25, 2004 PacketStorm, December 11, 2004 **Debian Security Advisory, DSA-609-1 atari800, December 14, 2004**
AtBas 2fax 3.04	A vulnerability was reported in 2fax. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted e-mail, web page, or other file that, when processed by the target user with 2fax, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the expandtabs() function in '2fax.c' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	AtBas 2fax expandtabs() Buffer Overflow	High	Secunia Advisory ID, SA13500, December 17, 2004
Bolthole Filter 2.6.1	A vulnerability exists in Filter that could allow a remote malicious user to cause arbitrary code to be executed by the target user. A remote user can send a specially crafted e-mail that, when processed by Filter, will execute arbitrary code on the target user's system. The code will run with the privileges of the Filter process. The buffer overflow resides in the save_embedded_address() function in 'filter.c.' The vendor plans to issue a fix in the pending version 2.6.2. A Proof of Concept exploit script has been published.	Bolthole Filter save_embedded _address() Buffer Overflow	High	SecurityTracker Alert ID, 1012560, December 16, 2004
BSD csv2xml 0.5.1	A vulnerability was reported in csv2xml. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted CSV file that, when processed by the target user with 'csv2xml -m=2,' will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the get_csv_token() function in 'csv2xml.cpp.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	BSD csv2xml get_csv_token() Buffer Overflow	High	SecurityTracker Alert ID, 1012582, December 16, 2004
BSD Junkie: 0.3.1	Two vulnerabilities were reported in Junkie. A remote server can cause arbitrary commands to be executed by the target user. A remote server can send a specially crafted FTP response to the connected Junkie client to execute arbitrary commands on the target user's system. The commands will run with the privileges of the target user. The flaws can be exploited if the target user selects 'View' or 'Download' for multiple files on the remote FTP server. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	BSD Junkie Input Validation Holes	High	SecurityTracker Alert ID, 1012571, December 16, 2004
BSD tnftp 20030825	A vulnerability was reported in tnftp. A remote server can write to arbitrary files on the target system. A remote FTP server can send a specially crafted FTP response to the connected tnftp client to write to arbitrary files on the target user's system with the privileges of the target user. The mget() function in 'cmds.c' does not validate server-supplied filenames and uses the server-supplied filename (including slashes) as a local filename. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	BSD tnftp mget() Input Validation Hole	High	Secunia Advisory ID, SA13516, December 17, 2004
Carsten Haitzler imlib 1.x	Multiple vulnerabilities exist due to integer overflows within the image decoding routines. This can be exploited to cause buffer overflows by tricking a user into viewing a specially crafted image in an application linked against the vulnerable library. Gentoo: http://security.gentoo.org/glsa/glsa-200412-03.xml **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-651.html** **SUSE:** **http://www.suse.com/en/private/download/updates** Currently we are not aware of any exploits for these vulnerabilities.	Carsten Haitzler imlib Image Decoding Integer Overflow CVE Name: CAN-2004-1026 CAN-2004-1025	High	Secunia Advisory ID, SA13381, December 7, 2004 Red Hat Advisory, RHSA-2004:651-03, December 10, 2004 **SecurityFocus, December 14, 2004**

Chris Walshaw abc2mtex 1.6.1	A vulnerability was reported in abc2mtex. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ABC file that, when processed by the target user with abc2mtex, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the process_abc() function in 'abc.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Chris Walshaw abc2mtex process_abc() Buffer Overflow	High	Secunia Advisory ID, SA13522, December 17, 2004
Christoph Appel Perl Crypt::ECB 1.1 -2, 1.1	A vulnerability exists because plain texts containing the ASCII character '0' is incorrectly encoded, which results in a weaker encryption and encoding collisions and may make it easier to brute force passwords. No workaround or patch available at time of publishing. There is no exploit code required; however; a Proof of Concept exploit has been published.	Christoph Appel Perl Crypt::ECB Incorrect Block Encryption	Medium	Securiteam, December 21, 2004
Christoph Dalitz abctab2ps 1.6.3	A vulnerability was reported in abctab2ps. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ABC file that, when processed by the target user with abctab2ps, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflows reside in the write_heading() function in 'subs.cpp' and the trim_title() function in 'parse.cpp.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Christoph Dalitz abctab2ps Buffer Overflows	High	SecurityTracker Alert ID, 1012578, December 16, 2004
Cscope Cscope 13.0, 15.1, 15.3-15.5	Several vulnerabilities exist: a vulnerability exists due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges; and a buffer overflow vulnerability exists when parsing source code with '#include' statements, which could let a malicious user execute arbitrary code. **SCO: UnixWare 7.1.4, 7.1.3, 7.1.1: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.21/erg712738.pkg.Z** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200412-11.xml** **Debian:** **http://www.debian.org/security/2004/dsa-610** Proofs of Concept exploits have been published.	Cscope Insecure Temporary File Creation & #include Statement Buffer Overflow CVE Name: CAN-2004-0996	Medium/ High (High if arbitrary code can be executed)	DV RX171104 Advisory, November 17, 2004 **SCO Security Advisory, SCOSA-2004.21, December 9, 2004** **Gentoo Linux Security Advisory, GLSA 200412-11 / cscope, December 16, 2004** **Debian Security Advisory DSA-610-1 cscope, December 17, 2004**
David Giffin xlreader 0.9.0	A buffer overflow vulnerability exists in book_format_sql() in 'format.c' that could allow a remote malicious user to execute arbitrary code on the target system. A remote user can create a specially crafted Excel document that, when processed via 'xlreader -s' by the target user, will trigger an overflow and execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	David Giffin xlreader book_format_sql() Buffer Overflow	High	SecurityTracker Alert ID, 1012540, December 16, 2004
Gastón Kleiman Yanf 0.4	A vulnerability exists that could allow a remote malicious user to cause arbitrary code to be executed by the target user. A remote server can send a specially crafted HTTP response to the connected Yanf client to execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the get() function in 'src/get.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Gastón Kleiman Yanf get() Buffer Overflow	High	SecurityTracker Alert ID, 1012557, December 16, 2004
GD Graphics Library gdlib 2.0.23, 2.0.26-2.0.28	A vulnerability exists in the 'gdImageCreateFromPngCtx()' function when processing PNG images due to insufficient sanity checking on size values, which could let a remote malicious user execute arbitrary code. OpenPKG: ftp://ftp.openpkg.org/release/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-08.xml Debian: http://security.debian.org/pool/updates/main/libg Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php	GD Graphics Library Remote Integer Overflow CVE Name: CAN-2004-0990 CAN-2004-0941	High	Secunia Advisory, SA12996, October 28, 2004 Gentoo Linux Security Advisory, GLSA 200411-08, November 3, 2004 Ubuntu Security Notice, USN-21-1, November 9, 2004 Debian Security Advisories, DSA 589-1 & 591-1, November 9, 2004 Fedora Update Notifications, FEDORA-2004-411 & 412, November 11, 2004 Mandrakelinux Security

	Trustix: http://http.trustix.org/pub/trustix/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool /updates/main/libg/libgd/ **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-638.html** An exploit script has been published.			Update Advisory, MDKSA-2004:132, November 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 Ubuntu Security Notice, USN-25-1, November 16, 2004 SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004 Debian Security Advisories, DSA 601-1 & 602-1, November 29, 2004 **Red Hat Advisory, RHSA-2004:638-09, December 17, 2004**
GNU a2ps 4.13	A vulnerability exists that could allow a malicious user to execute arbitrary shell commands on the target system. a2ps will execute shell commands contained within filenames. A user can create a specially crafted filename that, when processed by a2ps, will execute shell commands with the privileges of the a2ps process. A patch for FreeBSD is available at: http://www.freebsd.org/cgi/cvsweb.cgi/~checkout~/ports/ print/a2ps-letter/files/patch-select.c?rev=1.1&content-type=text/plain **Debian:** **http://www.debian.org/security/2004/dsa-612** A Proof of Concept exploit has been published.	GNU a2ps Filenames Shell Commands Execution	High	SecurityTracker Alert ID, 1012475, December 10, 2004 **Debian Security Advisory** **DSA-612-1 a2ps, December 20, 2004**
GNU Gentoo Aspell 0.50.5; Gentoo Linux 1.4	A buffer overflow vulnerability exists in the 'word-list-compress' utility due to insufficient bounds checking, which could let a malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200406-14.xml OpenPKG: ftp://ftp.openpkg.org/ Mandrakesoft: http://www.mandrakesoft.com/security/ advisories?name=MDKSA-2004:153 Proofs of Concept exploits have been published.	GNU Aspell Stack Buffer Overflow CVE Name: CAN-2004-0548	High	Securiteam, June 14, 2004 Gentoo Linux Security Advisory, GLSA 200406-14, June 17, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.042, September 15, 2004 Mandrakesoft Security Advisory MDKSA-2004:153, December 20, 2004
GNU ChBg 1.5	A vulnerability was reported in ChBg. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ChBg scenario file that, when processed by the target user with ChBg, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the simplify_path() function in 'config.c.' FreeBSD is not affected because PATH_MAX is set to 1024, preventing the buffer overflow. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	GNU ChBg simplify_path() Buffer Overflow	High	Secunia Advisory ID, SA13529, December 17, 2004
GNU Convex 3D 0.8pre1	A vulnerability exists that could allow a remote malicious user to cause arbitrary code to be executed by the target user. A remote user can create a specially crafted 3DS file that, when processed by the target user with Convex 3D, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the readObjectChunk() function in '3dsimp.cpp.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	GNU Convex 3D readObjectChunk() Buffer Overflow	High	SecurityTracker Alert ID, 1012555, December 16, 2004
GNU CUPS 1.1.22	A vulnerability was reported in CUPS in the processing of HPGL files. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted HPGL file that, when printed by the target user with CUPS, will execute arbitrary code on the target user's system. The code will run with the privileges of the 'lp' user. The buffer overflow resides	GNU CUPS HPGL ParseCommand() Buffer Overflow	High	CUPS Advisory STR #1023, December 16, 2004

	in the ParseCommand() function in 'hpgl-input.c.' Fixes are available in the CVS repository and are included in version 1.1.23rc1. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ A Proof of Concept exploit script has been published.			
GNU CUPS lppasswd 1.1.22	A vulnerability was reported in the CUPS lppasswd utility. A local malicious user can truncate or modify certain files and cause Denial of Service conditions on the target system. There are flaws in the way that lppasswd edits the '/usr/local/etc/cups/passwd' file. Fixes are available in the CVS repository and are included in version 1.1.23rc1. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ A Proof of Concept exploit has been published.	GNU CUPS lppasswd Denial of Service	Low	SecurityTracker Alert ID, 1012602, December 16, 2004
GNU DXFscope 0.2	A buffer overflow vulnerability exists in the dxfin() function in 'd.c' that could allow a remote malicious user to execute arbitrary code on the target system. A remote user can create a specially crafted DXF file that, when viewed by the target user with DXFscope, will execute arbitrary code on the target user's system. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	GNU DXFscope dxfin() Buffer Overflow	High	SecurityTracker Alert ID, 1012541, December 16, 2004
GNU jcabc2ps 20040902	A vulnerability was reported in jcabc2ps. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ABC file that, when processed by the target user with jcabc2ps, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the switch_voice() function in 'parse.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	GNU jcabc2ps switch_voice() Buffer Overflow	High	SecurityTracker Alert ID, 1012593, December 16, 2004
GNU jpegtoavi 1.5	A vulnerability exists that could allow a remote malicious user to cause arbitrary code to be executed by the target user. A remote user can create specially crafted JPEG files and a list of the JPEG filenames that, when processed by the target user with jpegtoavi, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the get_file_list_stdin() function in 'jpegtoavi.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	GNU jpegtoavi get_file_list_stdin() Buffer Overflow	High	SecurityTracker Alert ID, 1012559, December 16, 2004
GNU MPlayer 1.0pre5	A vulnerability was reported in MPlayer in the processing of ASF streams. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ASF video stream that, when viewed by the target user with MPlayer, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-21.xml A Proof of Concept exploit script has been published.	GNU MPlayer ASF Streams Processing Buffer Overflow	High	SecurityTracker Alert ID, 1012562, December 16, 2004 Gentoo GLSA 200412-21 / MPlayer, December 12, 2004
GNU NapShare 1.2	A vulnerability was reported in NapShare when used with an 'extern' filter. A remote malicious user can execute arbitrary code on the target user's system. A remote user can create a specially crafted gnutella response to NapShare that will execute arbitrary code on the target user's system. The buffer overflow resides in the auto_filter_extern() function in 'auto.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	GNU NapShare auto_filter_extern() Buffer Overflow	High	SecurityTracker Alert ID, 1012577, December 16, 2004
GNU pgn2web 0.3	A vulnerability was reported in pgn2web. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted PGN file that, when processed by the target user with pgn2web, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the process_moves() function in 'pgn2web.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	GNU pgn2web process_moves() Buffer Overflow	High	SecurityTracker Alert ID, 1012579, December 16, 2004
GNU rtf2latex2e 1.0fc2	A buffer overflow vulnerability exists that could allow a remote malicious user to execute arbitrary code on the target system. A remote user can create a specially crafted RTF file that, when processed by the target user with rtf2latex2e, will execute arbitrary code on the target user's system. The code will	GNU rtf2latex2e ReadFontTbl() Buffer Overflow	High	SecurityTracker Alert ID, 1012544, December 16, 2004

	run with the privileges of the target user. The buffer overflow resides in ReadFontTbl() in 'reader.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.			
GNU unrtf 0.19.3	A vulnerability was reported in unrtf. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted RTF file that, when processed by the target user with unrtf, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the process_font_table() function in 'convert.c.'. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	GNU unrtf process_font_table() Buffer Overflow	High	SecurityTracker Alert ID, 1012595, December 16, 2004
GNU Vim 6.x, GVim 6.x	Multiple vulnerabilities exist which can be exploited by local malicious users to gain escalated privileges. The vulnerabilities are caused due to some errors in the modelines options. This can be exploited to execute shell commands when a malicious file is opened. Successful exploitation can lead to escalated privileges but requires that modelines is enabled. Apply patch for vim 6.3: ftp://ftp.vim.org/pub/vim/patches/6.3/6.3.045 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-10.xml Currently we are not aware of any exploits for these vulnerabilities.	GNU Vim / Gvim Modelines Command Execution Vulnerabilities CVE Name: CAN-2004-1138	Medium	Gentoo Linux Security Advisory, GLSA 200412-10 / vim, December 15, 2004
GNU xine-lib 1.x	Multiple vulnerabilities with unknown impacts exist due to errors in the PNM and Real RTSP clients. Update to version 1-rc8: http://xinehq.de/index.php/download Currently we are not aware of any exploits for these vulnerabilities.	GNU xine-lib Unspecified PNM and Real RTSP Clients Vulnerabilities	Not Specified	Secunia Advisory, SA13496, December 16, 2004
GNU Yet Another MP3 Tool (YAMT) 0.5	A vulnerability was reported in Yet Another MP3 Tool (YAMT). A remote malicious user can cause arbitrary commands to be executed by the target user. A remote user can create a specially crafted MP3 file that, when processed by the target user with the YAMT Sort feature, will execute arbitrary commands on the target user's system. The commands will run with the privileges of the target user. The flaw resides in the id3tag_sort() function in 'id3tag.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU Yet Another MP3 Tool (YAMT) id3tag_sort() Input Validation Hole	High	SecurityTracker Alert ID, 1012583, December 16, 2004
GPL Xine 1-rc5, 1-rc7	A vulnerability was reported in Xine. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted file (such as an AVI file) that, when processed by the target user with Xine or xine-lib, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the open_aiff_file() function in 'demux_aiff.c.' A fix is available in the CVS repository. A Proof of Concept exploit script has been published.	GPL Xine open_aiff_file() Buffer Overflow	High	SecurityTracker Alert ID, 1012563, December 16, 2004
Guido Gonzato abcpp 1.3.0	A vulnerability was reported in abcpp. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ABC file that, when processed by the target user with abcpp, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the handle_directive() function in 'abcpp.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Guido Gonzato abcpp handle_directive() Buffer Overflow	High	Secunia Advisory ID, SA13524, December 17, 2004
Helmut Cantzler Mesh Viewer 0.2.2	A vulnerability was reported in Mesh Viewer. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted mesh file that, when processed by the target user with Mesh Viewer, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the Mesh::type() function in 'mesh.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Helmut Cantzler Mesh Viewer dxfin() Buffer Overflow	High	SecurityTracker Alert ID, 1012580, December 16, 2004
Hewlett-Packard HP-UX 11.x	A vulnerability exists which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is due to an unspecified error in the newgrp utility. Apply patches: http://www.itrc.hp.com/service/patch/mainPage.do Currently we are not aware of any exploits for this vulnerability.	HP-UX newgrp Privilege Escalation	Medium	Secunia Advisory ID, SA13565, December 20, 2004

html2hdml 1.0.3	A vulnerability was reported in html2hdml. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted HTML file that, when processed by the target user with html2hdml, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the remove_quote() function in 'convert.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	html2hdml remove_quote() Buffer Overflow	High	SecurityTracker Alert ID, 1012590, December 16, 2004
IBM AIX 5.x	Multiple vulnerabilities exist in AIX, which can be exploited by malicious, local users to gain escalated privileges. These vulnerabilities exist in the 'paginit' utility, the '/bin/Dctrl' utility, the 'uname' utility, and the 'grep' utility. Successful exploitation of the vulnerabilities allows execution of arbitrary code with 'root' privileges. Apply APARs: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp Currently we are not aware of any exploits for these vulnerabilities.	IBM AIX Multiple Privilege Escalation Vulnerabilities	High	iDEFENSE Security Advisory 12.20.04
IglooFTP IglooFTP 0.6.1	A vulnerability was reported in IglooFTP. A remote server can write to arbitrary files on the target system. A remote FTP server can send a specially crafted FTP response to the connected IglooFTP client to write to arbitrary files on the target user's system with the privileges of the target user. The download_selection_recursive() function in 'ftplist.c' does not validate server-supplied filenames and uses the server-supplied filename as a local filename. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	IglooFTP download_selection_recursive() Input Validation Hole	High	SecurityTracker Alert ID, 1012588, December 16, 2004
Info-ZIP Zip 2.3	A buffer overflow vulnerability exists due to a boundary error when doing recursive compression of directories with 'zip,' which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zip/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-634.html** Currently we are not aware of any exploits for this vulnerability.	Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow CVE Name: CAN-2004-1010	High	Bugtraq, November 3, 2004 Ubuntu Security Notice, USN-18-1, November 5, 2004 Fedora Update Notification, FEDORA-2004-399 & FEDORA-2004-400, November 8 & 9, 2004 Gentoo Linux Security Advisory, GLSA 200411-16, November 9, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:141, November 26, 2004 SUSE Security Summary Report, SUSE-SR:2004:003, December 7, 2004 **Red Hat Advisory, RHSA-2004:634-08, December 16, 2004**
J Whitham HTGET 0.93	A buffer overflow vulnerability was reported in HTGET. A remote malicious user can cause arbitrary code to be executed. A remote user can create a specially crafted URL that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code. Debian: http://www.debian.org/security/2004/dsa-611 Currently we are not aware of any exploits for this vulnerability.	J Whitham HTGET Buffer Overflow CVE Name: CAN-2004-0852	High	Debian Security Advisory DSA-611-1 htget, December 20, 2004
Jean-François Moine abcm2ps 3.7.20	A vulnerability was reported in abcm2ps. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ABC file that, when processed by the target user with abcm2ps, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the put_words() function in 'subs.c.' Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-18.xml A Proof of Concept exploit script has been published.	Jean-François Moine abcm2ps put_words() Buffer Overflow	High	Secunia Advisory ID, SA13523, December 17, 2004 Gentoo Security Advisory, GLSA 200412-18 / abcm2ps, December 19, 2004

Jeff Dike uml_utilities 20030903	A vulnerability was reported in uml_utilities in the uml_net component. A local malicious user can disable the Ethernet interfaces on the target system. A local user can issue a specially crafted command to takedown an Ethernet interface. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Jeff Dike uml_utilities umt_net slip_down() Denial of Service	Low	SecurityTracker Alert ID, 1012603, December 16, 2004
KDE Konqueror prior to 3.32	Two vulnerabilities exist in KDE Konqueror, which can be exploited by malicious people to compromise a user's system.The vulnerabilities are caused due to some errors in the restriction of certain Java classes accessible via applets and Javascript. This can be exploited by a malicious applet to bypass the sandbox restriction and read or write arbitrary files. Update to version 3.3.2: http://kde.org/download/ Apply patch for 3.2.3: ftp://ftp.kde.org/pub/kde/security_patches/post-3.2.3-kdelibs-khtml-java.tar.bz2 Currently we are not aware of any exploits for these vulnerabilities.	KDE Konqueror Java Sandbox Vulnerabilities	High	KDE Security Advisory, December 20, 2004
KDE Konqueror 3.2.2-6	A vulnerability exists which can be exploited by malicious people to spoof the content of websites. A website can inject content into another site's window if the target name of the window is known. This can be exploited by a malicious website to spoof the content of a pop-up window opened on a trusted website. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **Mandrakesoft:** **http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:150** Currently we are not aware of any exploits for this vulnerability.	KDE Konqueror Window Injection **CVE Name:** **CAN-2004-1158**	Medium	Secunia Advisory ID, SA13254, December 8, 2004 **Secunia Advisory ID, SA13486, December 16, 2004** **Mandrakesoft Security Advisory, MDKSA-2004:150, December 15, 2004**
KDE KDE prior to 3.3.2	When a user creates a link to a remote file using various KDE applications, the resulting link may include authentication credentials for the remote system. This may include Samba passwords for files located on SMB servers. Patches are available: http://www.kde.org/info/security/advisory-20041209-1.txt **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200412-16.xml** Currently we are not aware of any exploits for this vulnerability.	KDE Privacy Vulnerability	Medium	KDE Security Advisory, December 9, 2004 **US-CERT Vulnerability Note VU#305294, December 17, 2004** **Gentoo Advisory, GLSA 200412-16 / KDE, December 19, 2004**
MIT Kerberos 5 krb5-1.3.5 and prior	A buffer overflow exists in the libkadm5srv administration library. A remote malicious user may be able to execute arbitrary code on an affected Key Distribution Center (KDC) host. There is a heap overflow in the password history handling code. A patch is available at: http://web.mit.edu/kerberos/advisories/2004-004-patch_1.3.5.txt Currently we are not aware of any exploits for this vulnerability.	Kerberos libkadm5srv Heap Overflow CVE Name: CAN-2004-1189	High	SecurityTracker Alert ID, 1012640, December 20, 2004
LGPL NASM 0.98.38	A vulnerability was reported in NASM. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted asm file that, when processed by the target user with NASM, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the error() function in 'preproc.c.' Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-20.xml A Proof of Concept exploit script has been published.	LGPL NASM error() Buffer Overflow	High	Secunia Advisory ID, SA13523, December 17, 2004
libtiff.org LibTIFF 3.6.1	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/	LibTIFF Buffer Overflows CVE Name: CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, October 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory,

	linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ KDE: Update to version 3.3.2: http://kde.org/download/ Apple Mac OS X: http://www.apple.com/swupdates/ **Gentoo: KDE kfax:** **http://www.gentoo.org/security/en/glsa/glsa-200412-17.xml** Proofs of Concept exploits have been published.			DSA 567-1, October 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:109 & MDKSA-2004:111, October 20 & 21, 2004 SuSE Security Announcement, SUSE-SA:2004:038, October 22, 2004 RedHat Security Advisory, RHSA-2004:577-16, October 22, 2004 Slackware Security Advisory, SSA:2004-305-02, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:888, November 8, 2004 US-CERT Vulnerability Notes VU#687568 & VU#948752, December 1, 2004 Gentoo Linux Security Advisory, GLSA 200412-02, December 6, 2004 KDE Security Advisory, December 9, 2004 Apple Security Update SA-2004-12-02 **Gentoo Security Advisory, GLSA 200412-17 / kfax, December 19, 2004**
Little Igloo LinPopUp 1.2.0	A buffer overflow vulnerability exists that could allow a remote malicious user to execute arbitrary code on the target system. A remote user can send a specially crafted message to LinPopUp to trigger a buffer overflow in strexpand() in 'string.c' and execute arbitrary code. The code will run with the privileges of the LinPopUp process. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Little Igloo LinPopUp strexpand() Buffer Overflow	High	SecurityTracker Alert ID, 1012542, December 16, 2004
Michael Hipp mpg123 0.59r	A vulnerability exists that could allow a remote malicious user to cause arbitrary code to be executed by the target user. A remote user can create a specially crafted MP3 playlist that, when processed by the target user with mpg123, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the find_next_file() function in 'playlist.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Michael Hipp mpg123 find_next_file() Buffer Overflow	High	Secunia Advisory ID, 13511, December 17, 2004
Michael Kohn Ringtone Tools 2.22	A vulnerability was reported in Ringtone Tools. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted eMelody file that, when processed by the target user with Ringtone Tools, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the parse_emelody() function in 'parse_emelody.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Michael Kohn Ringtone Tools parse_emelody() Buffer Overflow	High	SecurityTracker Alert ID, 1012573, December 16, 2004

Michael Kohn Visual Basic to C/GTK (vb2c) 0.02	A vulnerability was reported in Visual Basic to C/GTK (vb2c). A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted FRM file that, when processed by the target user with vb2c, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the gettoken() function in 'vb2c.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Michael Kohn Visual Basic to C/GTK (vb2c) gettoken() Buffer Overflow	High	SecurityTracker Alert ID, 1012575, December 16, 2004
Multiple Vendors ncpfs 2.2.1 - 2.2.4	A buffer overflow exists that could lead to local execution of arbitrary code with elevated privileges. The vulnerability is in the handling of the '-T' option in the ncplogin and ncpmap utilities, which are both installed as SUID root by default. Gentoo: Update to 'net-fs/ncpfs-2.2.5' or later http://www.gentoo.org/security/en/glsa/glsa-200412-09.xml Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors ncpfs: ncplogin and ncpmap Buffer Overflow CVE Name: CAN-2004-1079	High	Gentoo Linux Security Advisory, GLSA 200412-09 / ncpfs, December 15, 2004
Multiple Vendors Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; GNU Emacs 20.0-20.6, 21.2	A vulnerability exists in the Emacs flim library due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/f/flim/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-344.html Fedora Legacy: http://download.fedoralegacy.org/redhat/ **Fedora Core 2:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/** We are not aware of any exploits for this vulnerability.	Multiple Vendors Emacs flim Library Insecure Temporary File Creation CVE Name: CAN-2004-0422	Medium	Debian Security Advisory, DSA 500-1, May 2, 2004 Fedora Legacy Update Advisory, FLSA:1581, September 30, 2004 **Secunia Advisory ID: 13487, December 16, 2004**
Multiple Vendors file 4.11 and prior (Trustix)	A vulnerability exists in the ELF header parsing code in 'file'. A malicious user may be able to create a specially crafted ELF file that, when processed using 'file', may be able to modify the stack and potentially execute arbitrary code. Update to version 4.12: ftp://ftp.astron.com/pub/file/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-07.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/x86_64/update/9.0/rpm/x86_64/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors 'File' Processing ELF Headers Stack Overflow	High	Trustix Secure Linux Advisory #2004-0063, November 26, 2004 Gentoo Linux Security Advisory, GLSA 200412-07/ file, December 13, 2004 **SUSE Security Summary Report, SUSE-SR:2004:004, December 16, 2004**
Multiple Vendors glibc 2.2	A buffer overflow vulnerability exists in the resolver libraries of glibc 2.2. SUSE: ftp://ftp.SUSE.com/pub/SUSE **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-586.html** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors glibc Buffer Overflow CVE Name: CAN-2002-0029 **CAN-2004-0968**	Low	SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004 **Red Hat RHSA-2004:586-15, December 20, 2004**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.27	A vulnerability exists in the 'AF_UNIX' address family due to a serialization error, which could let a malicious user obtain elevated privileges or possibly execute arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 SUSE: ftp://ftp.SUSE.com/pub/SUSE **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main** **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel AF_UNIX Arbitrary Kernel Memory Modification CVE Name: CAN-2004-1068	Medium/ High (High if arbitrary code can be executed)	Bugtraq, November 19, 2004 SUSE Security Summary Report, SUSE-SR:2004:003, December 7, 2004 **SecurityFocus, December 14, 2004**

Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9	A vulnerability was reported in the Linux kernel in the auxiliary message (scm) layer. A local malicious user can cause Denial of Service conditions. A local user can send a specially crafted auxiliary message to a socket to trigger a deadlock condition in the __scm_send() function. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Multiple Vendors Linux Kernel Auxiliary Message Layer State Error CVE Name: CAN-2004-1016	Low	iSEC Security Research Advisory 0019, December 14, 2004
Multiple Vendors Unix Linux kernel 2.4, 2.4 .0-test1 test12, 2.4.1 2.4.25, 2.6, test1 test11, 2.6.1 -rc1&rc2, 2.6.2 2.6.4	A vulnerability exists in the Linux kernel when writing to an ext3 file system due to a design error that causes some kernel information to be leaked, which could let a malicious user obtain sensitive information. Upgrade available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 Conectiva: ftp://ul.conectiva.com.br/updates/1.0/ Debian: http://security.debian.org/pool/updates/main/k/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **RedHat (updated kernel package): http://rhn.redhat.com/errata/RHSA-2004-504.html** Trustix: http://http.trustix.org/pub/trustix/updates/ Engarde: http://infocenter.guardiandigital.com/advisories/	Multiple Vendors Linux Kernel EXT3 File System Information Leakage CVE Name: CAN-2004-0177	Medium	Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004 Debian Security Advisories, DSA 489-1 & 491-1, April 17, 2004 Conectiva Security Advisory, CLSA-2004:829, April 15, 2004 Red Hat Security Advisories, RHSA-2004:166-01 & 166-08, April 21, 2004 Guardian Digital Security Advisory, ESA-20040428-004, April 28, 2004 **Red Hat Security Advisories, RHSA-2004:505-14 & 505-13, December 13, 2004**
Multiple Vendors Linux Kernel 2.4.x	The Linux kernel is reported prone to a data disclosure vulnerability. It is reported that this issue may permit a malicious executable to disclose the contents of Floating Point registers that belong to another process. This vulnerability will only affect ia64 systems. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.securityfocus.com/advisories/6925 Gentoo: http://www.securityfocus.com/advisories/6969 **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Floating Point Register Contents Leak CVE Name: CAN-2004-0565	Medium	Trustix Secure Linux, TSLSA-2004-0041 Mandrake MDKSA-2004:066 Gentoo GLSA 200407-16 **Red Hat Linux RHSA-2004:504-13, December 13, 2004**
Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9	Several vulnerabilities exist in the Linux kernel in the processing of IGMP messages. A local user may be able to gain elevated privileges. A remote user can cause the target system to crash. These are due to flaws in the ip_mc_source() and igmp_marksources() functions. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Multiple Vendors Linux Kernel IGMP Integer Underflow CVE Name: CAN-2004-1137	Low/ Medium (Medium if elevated privileges can be obtained)	iSEC Security Research Advisory 0018, December 14, 2004
Multiple Vendors Linux Kernel 2.6 - 2.6.9, 2.4 - 2.4.28	Integer overflow vulnerabilities exist that could allow a local user to cause Denial of Service conditions. These overflows exist in ip_options_get() and vc_resize() and a memory leak in ip_options_get(). The vendor has issued a fix in 2.6.10rc3bk5 and possibly also in the 2.4 release candidate. A Proof of Concept exploit has been published.	Multiple Vendors Linux Kernel ip_options_get() and vc_resize() Integer Overflows	Low	Georgi Guninski Security Advisory #72, December 15, 2004
Multiple Vendors Linux kernel 2.6.x, 2.4.x , SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x,	Two vulnerabilities exist: a Denial of Service vulnerability exists via a specially crafted 'a.out' binary; and a vulnerability exists due to a race condition in the memory management, which could let a malicious user obtain sensitive information. SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html	Multiple Vendors Linux Kernel Local DoS & Memory Content Disclosure CVE Name: CAN-2004-1074	Low/ Medium (Medium if sensitive information	Secunia Advisory, SA13308, November 25, 2004 SUSE Security Summary Report, SUSE-SA:2004:042,

SUSE Linux Enterprise Server 8, 9; Turbolinux Turbolinux Server 10.0	**TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/RPMS/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/** Currently we are not aware of any exploits for these vulnerabilities.		can be obtained)	December 1, 2004 **SecurityFocus, December 16, 2004**
Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The DRM module in the Linux kernel is susceptible to a local Denial of Service vulnerability. This vulnerability likely results in the corruption of video memory, crashing the X server. Malicious users may be able to modify the video output. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Local DRM Denial of Service CVE Name: CAN-2004-1056	Low	Ubuntu Security Notice USN-38-1 December 14, 2004
Multiple Vendors Unix Linux kernel 2.4, 2.4 .0-test1 test12, 2.4.1 2.4.25, 2.6, test1 test11, 2.6.1 -rc1&rc2, 2.6.2 2.6.4	Multiple vulnerabilities exist: a vulnerability exists due to information leaks within the JFS file system code, which could let a malicious user obtain sensitive information; and a Denial of Service vulnerability exists in the Linux Sound Blaster driver. Upgrade available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: http://www.turbolinux.com/security/ **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel Multiple Vulnerabilities CVE Names: CAN-2004-0178 CAN-2004-0181	Low/ Medium (Medium if sensitive information can be obtained)	Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004 SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004 Turbolinux, TLSA-2004-05-21, May 21, 2004 **Red Hat Advisory ID: RHSA-2004:504-13, December 13, 2004**
Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The Linux kernel /proc filesystem is susceptible to an information disclosure vulnerability. This issue is due to a race-condition allowing unauthorized access to potentially sensitive process information. This vulnerability may allow malicious local users to gain access to potentially sensitive environment variables in other users processes. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel PROC Filesystem Local Information Disclosure CVE Name: CAN-2004-1058	Medium	Ubuntu Security Notice USN-38-1 December 14, 2004
Multiple Vendors Linux kernel 2.6.8 rc1-rc3	A Denial of Service vulnerability exists in the 'ReiserFS' file system functionality due to a failure to properly handle files under certain conditions. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.9.tar.bz2 **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/** There is no exploit code required.	Multiple Vendors Linux Kernel ReiserFS File System Local Denial of Service CVE Name: CAN-2004-0814	Low	SecurityFocus, October 26, 2004 **Ubuntu Linux Security Advisory USN-38-1, December 14, 2004**
Multiple Vendors Linux Kernel 2.6 - 2.6.10 rc2	The Linux kernel is prone to a local Denial of Service vulnerability. This vulnerability is reported to exist when 'CONFIG_SECURITY_NETWORK=y' and 'CONFIG_SECURITY_SELINUX=y' options are set in the Linux kernel. A local attacker may exploit this vulnerability to trigger a kernel panic and effectively deny service to legitimate users. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Sock_DGram_SendMsg Local Denial of Service CVE Name: CAN-2004-1069	Low	Ubuntu Security Notice USN-38-1 December 14, 2004

Multiple Vendors Linux Kernel 2.6.x	Some potential vulnerabilities exist with an unknown impact in the Linux Kernel. The vulnerabilities are caused due to boundary errors within the 'sys32_ni_syscall()' and 'sys32_vm86_warning()' functions and can be exploited to cause buffer overflows. **Immediate consequences of exploitation of this vulnerability could be a kernel panic. It is not currently known whether this vulnerability may be leveraged to provide for execution of arbitrary code.** Patches are available at: http://linux.bkbits.net:8080/linux-2.6/cset@1.2079 http://linux.bkbits.net:8080/linux-2.6/gnupatch@41ae6af1cR3mJYlW6D8EHxCKSxuJiQ Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel 'sys32_ni_syscall' and 'sys32_vm86_warning' Buffer Overflows **CVE Name:** **CAN-2004-1151**	Low/High (High if arbitrary code can be executed)	Secunia Advisory ID, SA13410, December 9, 2004 **SecurityFocus, December 14, 2004**
Multiple Vendors Linux Kernel versions except 2.6.9	A race condition vulnerability exists in the Linux Kernel terminal subsystem. This issue is related to terminal locking and is exposed when a remote malicious user connects to the computer through a PPP dialup port. When the remote user issues the switch from console to PPP, there is a small window of opportunity to send data that will trigger the vulnerability. This may cause a Denial of Service. This issue has been addressed in version 2.6.9 of the Linux Kernel. Patches are also available for 2.4.x releases: http://www.kernel.org/pub/linux/kernel/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel Terminal Locking Race Condition CVE Name: CAN-2004-0814	Low	SecurityFocus, December 14, 2004
Multiple Vendors Linux Kernel versions except 2.6.9	The Linux Kernel is prone to a local vulnerability in the terminal subsystem. Reportedly, this issue can be triggered by issuing a TIOCSETD ioctl to a terminal interface at the moment a read or write operation is being performed by another thread. This could result in a Denial of Service or allow kernel memory to be read. This issue has been addressed in version 2.6.9 of the Linux Kernel. Patches are also available for 2.4.x releases: http://www.kernel.org/pub/linux/kernel/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel TIOCSETD Terminal Subsystem Race Condition CVE Name: CAN-2004-0814	Low	SecurityFocus, December 14, 2004
Multiple Vendors Linux Kernel USB Driver prior to 2.4.27	A vulnerability exists in certain USB drivers because uninitialized structures are used and then 'copy_to_user(...)' kernel calls are made from these structures, which could let a malicious user obtain obtain uninitialized kernel memory contents. Update available at: http://kernel.org/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200408-24.xml Trustix: http://http.trustix.org/pub/trustix/updates/ **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html** We are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Kernel USB Driver Kernel Memory CVE Name: CAN-2004-0685	Medium	US-CERT Vulnerability Note VU#981134, October 25, 2004 Trustix, TSLSA-2004-0041: kernel, August 9, 2004 **Red Hat Security Advisories, RHSA-2004:505-14 & 505-13, December 13, 2004**
Multiple Vendors nfs-utils 1.0.6	A vulnerability exists due to an error in the NFS statd server in 'statd.c' where the 'SIGPIPE' signal is not correctly ignored. This can be exploited to crash a vulnerable service via a malicious peer terminating a TCP connection prematurely. Upgrade to 1.0.7-pre1: http://sourceforge.net/project/showfiles.php?group_id=14&package_id=174 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:146 Debian: http://www.debian.org/security/2004/dsa-606 **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-583.html** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors nfs-utils 'SIGPIPE' TCP Connection Termination Denial of Service **CVE Name:** **CAN-2004-0946** **CAN-2004-1014**	Low	Secunia Advisory ID, SA13384, December 7, 2004 Debian Security Advisory DSA-606-1 nfs-utils, December 8, 2004 **Red Hat Security Advisory, RHSA-2004:583-09, December 20, 2004**

Multiple Vendors Samba 2.2.9, 3.0.8 and prior	An integer overflow vulnerability in all versions of Samba's smbd 0.8 could allow an remote malicious user to cause controllable heap corruption, leading to execution of arbitrary commands with root privileges. Patches available at: http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch Red Hat: http://rhn.redhat.com/errata/RHSA-2004-670.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-13.xml Trustix: http://www.trustix.net/errata/2004/0066/ Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Samba smbd Security Descriptor CVE Name: CAN-2004-1154	High	iDEFENSE Security Advisory 12.16.04 Red Hat Advisory, RHSA-2004:670-10, December 16, 2004 Gentoo Security Advisory, GLSA 200412-13 / Samba, December 17, 2004 US-CERT, Vulnerability Note VU#226184, December 17, 2004 Trustix Secure Linux Advisory #2004-0066, December 17, 2004
Multiple Vendors Samba 3.0 - 3.0.7; RedHat Advanced Workstation for the Itanium Processor 2.1, IA64, Desktop 3.0, Enterprise Linux WS 3, WS 2.1 IA64, 2.1, ES 3, 2.1 IA64, 2.1, AS 3, 2.1 IA64, 2.1; Ubuntu Linux 4.1 ppc, ia64, ia32	A buffer overflow vulnerability exists in the 'QFILEPATHINFO' request handler when constructing 'TRANSACT2_QFILEPATHINFO' responses, which could let a remote malicious user execute arbitrary code. Update available at: http://www.samba.org/samba/download/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: Ubuntu Upgrade samba-doc_3.0.7-1ubuntu6.2_all.deb Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/ **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-632.html** **OpenPKG:** **http://www.openpkg.org/security.html** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Samba 'QFILEPATHINFO' Buffer Overflow CVE Name: CAN-2004-0882	High	e-matters GmbH Security Advisory, November 14, 2004 SuSE Security Announcement, SUSE-SA:2004:040, November 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 Ubuntu Security Notice, USN-29-1, November 18, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:136, November 19, 2004 US-CERT Vulnerability Note VU#457622, November 19, 2004 Conectiva Linux Security Announcement, CLA-2004:899, November 25, 2004 Fedora Update Notifications, FEDORA-2004-459 & 460, November 29, 2004 Turbolinux Security Advisory, TLSA-2004-32, December 8, 2004 **Red Hat Security Advisory RHSA-2004:632-17, November 16, 2004** **OpenPKG Security Advisory, OpenPKG-SA-2004.054 December 17, 2004**

Multiple Vendors Gentoo Linux; Samba Samba 3.0-3.0.7	A remote Denial of Service vulnerability exists in 'ms_fnmatch()' function due to insufficient input validation. Patch available at: http://us4.samba.org/samba/ftp/patches/security/samba-3.0.7-CAN-2004-0930.patch Gentoo: http://security.gentoo.org/glsa/glsa-200411-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/samba/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-632.html Trustix: http://http.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SGI: http://www.sgi.com/support/security/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/ **OpenPKG:** **http://www.openpkg.org/security.html** There is no exploit code required.	Multiple Vendors Samba Remote Wild Card Denial of Service CVE Name: CAN-2004-0930	Low	SecurityFocus, November 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 RedHat Security Advisory, RHSA-2004:632-17, November 16, 2004 Conectiva Linux Security Announcement, CLA-2004:899, November 25, 2004 Fedora Update Notifications, FEDORA-2004-459 & 460, November 29, 2004 Turbolinux Security Advisory, TLSA-2004-32, December 8, 2004 SGI Security Advisory, 20041201-01-P, December 13, 2004 **OpenPKG Security Advisory, OpenPKG-SA-2004.054 December 17, 2004**
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.8 SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9	Multiple vulnerabilities exist due to various errors in the 'load_elf_binary' function of the 'binfmt_elf.c' file, which could let a malicious user obtain elevated privileges and potentially execute arbitrary code. Patch available at: http://linux.bkbits.net:8080/linux-2.6/gnupatch@41925edcVccsXZXObG444GFvEJ94GQ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html Red Hat: http://rhn.redhat.com/errata/RHSA-2004-549.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html** **http://rhn.redhat.com/errata/RHSA-2004-505.html** Proofs of Concept exploit scripts have been published.	Multiple Vendors Linux Kernel BINFMT_ELF Loader Multiple Vulnerabilities CVE Names: CAN-2004-1070 CAN-2004-1071 CAN-2004-1072 CAN-2004-1073	Medium/ High (High if arbitrary code can be executed)	Bugtraq, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 Red Hat Advisory: RHSA-2004:549-10, December 2, 2004 **RedHat Security Advisories, RHSA-2004:504-13 & 505-14, December 13, 2004**

Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.9; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32; SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9	Multiple remote Denial of Service vulnerabilities exist in the SMB filesystem (SMBFS) implementation due to various errors when handling server responses. This could also possibly lead to the execution of arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html Red Hat: http://rhn.redhat.com/errata/RHSA-2004-549.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html** **http://rhn.redhat.com/errata/RHSA-2004-505.html** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/** Currently we are not aware of any exploits for these vulnerabilities	Multiple Vendors smbfs Filesystem Memory Errors Remote Denial of Service CVE Names: CAN-2004-0883 CAN-2004-0949	Low/High (High if arbitrary code can be executed)	e-matters GmbH Security Advisory, November 11, 2004 Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004 SUSE Security Summary Report, SUSE-SA:2004:042, December 1, 2004 Red Hat Advisory: RHSA-2004:549-10, December 2, 2004 **Ubuntu Security Notice, USN-39-1, December 16, 2004** **RedHat Security Advisories, RHSA-2004:504-13 & 505-14, December 13, 2004**
Namazu Project Namazu 2.0.13 and prior	A vulnerability exists which can be exploited by malicious people to conduct Cross-Site Scripting attacks. Input passed to 'namazu.cgi' isn't properly sanitized before being returned to the user if the query begins from a tab ('%09'). This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Update to version 2.0.14: http://namazu.org/#download Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.	Namazu Cross-Site Scripting Vulnerability	High	Namazu Security Advisory, December 15, 2004
NetBSD Foundation NetBSD prior to 2.0	A vulnerability exists in the compat functions. A local malicious user can cause Denial of Service conditions or potentially gain elevated privileges. Some of the functions in /usr/src/sys/compat/* do not properly validate user-supplied data before executing a kernel syscall. Several functions do not properly validate signal numbers. A local malicious user can cause large signal numbers to be passed to certain syscall functions to cause the kernel to crash. Several buffer overflows exist. At least one of the buffer overflows allows a local user to gain root privileges. Version 2.0 includes the fix. Instructions on upgrading kernel binaries are provided in the vendor's advisory, available at: http://www.netbsd.org/Security/ Currently we are not aware of any exploits for these vulnerabilities.	NetBSD compat Validation Flaws	Low/ Medium/ High (Low of a DoS; Medium if elevated privileges can be obtained; and High if root privileges can be obtained)	SecurityTracker Alert ID, 1012611, December 17, 2004
o3read 0.0.3	A vulnerability was reported in o3read. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted SXW file that, when processed by the target user with o3read, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the parse_html() function in 'o3read.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	o3read parse_html() Buffer Overflow	High	SecurityTracker Alert ID, 1012591, December 16, 2004
Open Source Technology Group Slash CVS versions prior to R_2_5_0_41	A vulnerability with an unknown impact has been reported in slash. The vulnerability is caused due to an unspecified error in the CVS versions. Solution: Upgrade to Slash CVS version R_2_5_0_41 and release version 2.2.6: http://www.slashcode.com/slash/04/12/15/1540200.shtml?tid=11&tid=5&tid=4 Currently we are not aware of any exploits for this vulnerability.	Open Source Technology Slash Unspecified Vulnerability	Not Specified	Security Advisory for CVS Slash, December 15, 2004

OpenBSD Project OpenBSD 3.4, 3.5, 3.6	A vulnerability exists in isakmpd(8) which could allow a local malicious user to trigger a kernel panic. If the target system is running isakmpd(8), a local user can set ipsec(4) credentials on a socket to corrupt kernel memory and cause the system to panic. The flaw resides in the pfkeyv2_acquire() function in 'sys/net/pfkeyv2.c.' The vendor has issued a fix in OpenBSD-current and the OpenBSD 3.6, 3.5, and 3.4 -stable branches. Patches are also available for OpenBSD 3.6, 3.5 and 3.4: ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/ Currently we are not aware of any exploits for this vulnerability.	OpenBSD isakmpd Error in pfkeyv2_acquire()	Low	OpenBSD 3.6 release errata & patch list, December 14, 2004
Patric Müller Vilistextum 2.6.6	A vulnerability was reported in Vilistextum that could allow a remote malicious user to cause arbitrary code to be executed by the target user. A remote user can create a specially crafted HTML file that, when processed by the target user with Vilistextum, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflow resides in the get_attr() function in 'html.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Patric Müller Vilistextum get_attr() Buffer Overflow	High	SecurityTracker Alert ID, 1012558, December 16, 2004
PHPGroupWare PHPGroupWare 0.9.16.03	PHPGroupWare contains multiple input validation vulnerabilities; it is prone to multiple SQL injection and Cross-Site Scripting issues. These issues are all due to a failure of the application to properly sanitize user-supplied input. A malicious user could exploit these vulnerabilities to execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PHPGroupWare Multiple Cross-Site Scripting and SQL Injection	High	GulfTech Security Research December 14th, 2004
PHPGroupWare phpMyAdmin 2.4.0 up to 2.6.1-rc1	Two vulnerabilities exist which can be exploited by malicious people to compromise a vulnerable system and by malicious users to disclose sensitive information.1) An input validation error in the handling of MySQL data allows injection of arbitrary shell commands. 2) Input passed to 'sql_localfile' is not properly sanitized in 'read_dump.php' before being used to disclose files. Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-19.xml A Proof of Concept exploit has been published.	PHPGroupWare phpMyAdmin Two Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Exaprobe, Security Advisory, December 13, 2004
PostgreSQL PostgreSQL 7.4.5	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-16.xml Debian: http://security.debian.org/pool/updates/main/p/postgresql/ OpenPKG: ftp://ftp.openpkg.org/release/ Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:149 **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-489.html** There is no exploit code required.	PostgreSQL Insecure Temporary File Creation CVE Name: CAN-2004-0977	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory, GLSA 200410-16, October 18, 2004 Debian Security Advisory, DSA 577-1, October 29, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.046, October 29, 2004 Mandrakesoft Security Advisory, MDKSA-2004:149, December 13, 2004 **Red Hat Advisory RHSA-2004:489-17, December 20, 2004**
Red Hat Linux Kernel 2.4.x, ia64	A vulnerability exists in the Linux kernel, which potentially can be exploited to gain knowledge of sensitive information. The vulnerability is caused due to an error within the context switch code. Updates available at: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=124734 **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html** A Proof of Concept exploit has been published.	Red Hat Information leak on Linux/ia64 CVE Name: CAN-2004-0565	Medium	Bugzilla Bug 124734, May 28, 2004 **RedHat Security Advisory, RHSA-2004:504-13, December 13, 2004**

Roxio Toast 6.0 Titanium	A local privilege escalation vulnerability reportedly affects Roxio Toast. This issue is due to a design error in the application that allows an attacker to execute code with kernel privileges. A local attacker may leverage this issue to execute arbitrary code on the affected computer with superuser privileges, facilitating privilege escalation. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Roxio Toast TDIXSupport Local Privilege Escalation	High	SecurityFocus Bugtraq ID, 11940, December 15, 2004
Russell Marks xzgv .8	An integer overflow vulnerability exists in the processing of PRF files. A remote malicious user may be able to cause arbitrary code to be executed on the target user's computer. A remote user can create a specially crafted image file that, when processed by the target user, will trigger an overflow in the read_prf_file() function. The flaw resides in 'src/readprf.c', where image height and width parameters are not properly limited. A patch is available at: http://rus.members.beeb.net/xzgv-0.8-integer-overflow-fix.diff **Debian:** **http://www.debian.org/security/2004/dsa-614** Currently we are not aware of any exploits for this vulnerability.	Russell Marks xzgv Integer Overflow CVE Name: CAN-2004-0994	High	iDEFENSE Security Advisory, December 13, 2004 **Debian Security Advisory DSA-614-1 xzgv, December 21, 2004**
Russell Marks zgv Image Viewer 5.5	Several vulnerabilities exist due to various integer overflows when processing images, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200411-12.xml **Debian:** **http://www.debian.org/security/2004/dsa-608** **The vendor has issued a patch, available at: http://www.svgalib.org/rus/zgv/zgv-5.8-integer-overflow-fix.diff** Currently we are not aware of any exploits for these vulnerabilities.	Russell Marks ZGV Image Viewer Multiple Remote Integer Overflow **CVE Name:** **CAN-2004-1095** **CAN-2004-0999**	High	Bugtraq, October 26, 2004 Gentoo Linux Security Advisory, GLSA 200411-12:01, November 7, 2004 **Debian Security Advisory, DSA-608-1 zgv, December 14, 2004** **SecurityTracker Alert ID: 1012546, December 16, 2004**
Samba.org Samba version 3.0 - 3.0.6	Several vulnerabilities exist: a remote Denial of Service vulnerability exists in the 'process_logon_packet()' function due to insufficient validation of 'SAM_UAS_CHANGE' request packets; and a remote Denial of Service vulnerability exists when a malicious user submits a malformed packet to a target 'smbd' server. Updates available at: http://samba.org/samba/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/ SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-467.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** We are not aware of any exploits for these vulnerabilities.	Samba Remote Denials of Service CVE Names: CAN-2004-0807 CAN-2004-0808	Low	Securiteam, September 14, 2004 Gentoo Linux Security Advisory, GLSA 200409-16, September 13, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:092, September 13, 2004 Trustix Secure Linux Bugfix Advisory, TSL-2004-0046, September 14, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.040, September 15, 2004 SUSE Security Announcement, SUSE-SA:2004:034, September 17, 2004 RedHat Security Advisory, RHSA-2004:467-08, September 23, 2004 Conectiva Linux Security Announcement, CLA-2004:873, October 14, 200 **SGI Security Advisory, 20041201-01-P, December 13, 2004**

Seymour Shlien abcMIDI 2004.12.04	A vulnerability was reported in abcMIDI in the 'abc2midi' component. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted ABC file that, when processed by the target user with abc2midi, will execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The buffer overflows reside in the event_text() and event_specific() functions in 'store.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Seymour Shlien abcMIDI dxfin() Buffer Overflow	High	Secunia Advisory ID: SA13512, December 17, 2004
SGI IRIX 6.5.20 m, 6.5.20 f, 6.5.21 m, 6.5.21 f, 6.5.22-6.5.25	Several vulnerabilities exist: a Denial of Service vulnerability exists when a 'mapelf32exec()' call is made on a malicious binary; and a Denial of Service vulnerability exists due to page invalidation issues that exist in init. Patches available at: ftp://patches.sgi.com/support/free/security/advisories/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html** Currently we are not aware of any exploits for these vulnerabilities.	SGI IRIX Denials of Service CVE Names: CAN-2004-0136 CAN-2004-0137	Low	SGI Security Advisory, 20040601-01-P, June 14, 2004 **RedHat Security Advisory, RHSA-2004:504-13, December 13, 2004**
SGI Samba on SGI IRIX 6.5.x	Multiple vulnerabilities exist which can be exploited to cause a Denial of Service or compromise a vulnerable system. Apply patch 5798 for Samba 3.0.7: ftp://patches.sgi.com/support/free/security/advisories/20041201-01-P.asc **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2004-504.html and http://rhn.redhat.com/errata/RHSA-2004-549.html** Currently we are not aware of any exploits for these vulnerabilities.	SGI Multiple Samba Vulnerabilities CVE Names: CAN-2004-0807 CAN-2004-0882 CAN-2004-0930	Low/High (High if arbitrary code can be executed)	Samba Security Vulnerability Number, 20041201-01-P, December 7, 2004 **Red Hat Security Advisory, RHSA-2004:504-13, December 13, 2004** **Red Hat Security Advisory, RHSA-2004:549-10, December 2, 2004**
SQLgrey Postfix Greylisting Service 1.1.1, 1.1.3, 1.2 .0, 1.3 .0	A vulnerability exists due to insufficient sanitization of an unspecified input, which could let a remote malicious manipulate data. Upgrade available at: http://prdownloads.sourceforge.net/sqlgrey/sqlgrey-1.4.0.tar.bz2?download There is no exploit required.	SQLgrey Postfix Greylisting Service SQL Injection	Medium	Secunia Advisory, SA13431, December 13, 2004
Stuart Cunningham libbsb 0.0.6	A buffer overflow vulnerability exists that could allow a remote malicious user to execute arbitrary code on the target system. A remote user can create a specially crafted BBS image file that, when processed with bsb2ppm by the target user, will trigger an overflow and execute arbitrary code. The code will run with the privileges of the target user. The overflow resides in bsb_open_header() in 'bsb_io.c.' No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Stuart Cunningham libbsb bsb2ppm bsb_open_header() Buffer Overflow	High	SecurityTracker Alert ID, 1012543, December 16, 2004
Sun Microsystems iPlanet Messaging Server/Sun ONE Messaging Server	A input validation vulnerability may allow a remote malicious unprivileged user the ability to direct a local user's browser (Internet Explorer) to execute javascript to gain unauthorized access by using a specially crafted e-mail message. This issue only occurs when the client browser is Internet Explorer (IE). Updates available: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57691-1 Currently we are not aware of any exploits for this vulnerability.	Sun Security Vulnerability in Webmail	High	Sun Alert ID, 57691, December 15, 2004
Vinicius M. de Souza ChangePassword 0.8	A vulnerability was reported in ChangePassword. A local malicious user can obtain root privileges on the target system. A local user can invoke 'changepassword.cgi' on UNIX-based systems to execute arbitrary commands with root privileges. The script is installed with set user id (setuid) root user privileges by default. The script does not validate user-supplied environment variables, so a local user can set the PATH to point to a specially crafted version of 'make' and then submit a POST request directly to the application via the environment (rather than via HTTP) to execute the make application with root privileges. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Vinicius M. de Souza ChangePassword Root Privileges	High	SecurityTracker Alert ID, 1012601, December 16, 2004

xmlsoft.org Libxml2 2.6.12-2.6.14	Multiple buffer overflow vulnerabilities exist: a vulnerability exists in the 'xmlNanoFTPScanURL()' function in 'nanoftp.c' due to a boundary error, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'xmlNanoFTPScanProxy()' function in 'nanoftp.c,' which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handling of DNS replies due to various boundary errors, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://xmlsoft.org/sources/libxml2-2.6.15.tar.gz OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-05.xml Mandrake: http://www.mandrakesoft.com/security/advisories OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: http://www.trustix.org/errata/2004/0055/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libx/libxml2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-615.html Conectiva: ftp://atualizacoes.conectiva.com.br/1 **RedHat (libxml):** **http://rhn.redhat.com/errata/RHSA-2004-650.html** An exploit script has been published.	xmlsoft.org Libxml2 Multiple Remote Stack Buffer Overflows CVE Name: CAN-2004-0989 CAN-2004-0110	High	SecurityTracker Alert I, 1011941, October 28, 2004 Fedora Update Notification, FEDORA-2004-353, November 2, 2004 Gentoo Linux Security Advisory, GLSA 200411-05, November 2,2004 Mandrakelinux Security Update Advisory, MDKSA-2004:127, November 4, 2004 OpenPKG Security Advisory, OpenPKG-SA-2004.050, November 1, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0055, November 1, 2004 Ubuntu Security Notice, USN-10-1, November 1, 2004 Red Hat Security Advisory, RHSA-2004:615-11, November 12, 2004 Conectiva Linux Security Announcement, CLA-2004:890, November 18, 2004 **Red Hat Security Advisory, RHSA-2004:650-03, December 16, 2004**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
3Com 3CDaemon 2.0 revision 10	A remote Denial of Service vulnerability exists in the TFTP service when any command is invoked that contains a superfluous filename parameter. No workaround or patch available at time of publishing. There is no exploit code required.	3Com 3CDaemon TFTP Service Remote Denial of Service	Low	Bugtraq, December 15, 2004
68 Designs Froogle 1.x	A vulnerability exists in the default installation in the 'setup.php' script, which could let a remote malicious user obtain administrative access; and a vulnerability exists because a remote malicious user can invoke the 'setup.php' script to obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	68 Designs Froogle Installation Security Issue	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA13504, December 17, 2004
Adobe Systems Incorporated Acrobat 6.0-6.0.2, Acrobat Reader 6.0-6.0.2	A format string vulnerability exists in the in the ETD file parser when processing tag values, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.adobe.com/support/downloads/ Proofs of Concept exploits have been published.	Adobe Acrobat/Acrobat Reader ETD File Parser Format String CVE Name: CAN-2004-1153	High	iDEFENSE Security Advisory, December 14, 2004
Albrecht Guenther PHProjekt 2.0, 2.0.1, 2.1 a, 2.1-2.4, 3.0-3.2,	A vulnerability exists in 'setup.php' because arbitrary PHP scripts can be uploaded, including operating system commands, which could let a remote malicious user modify the configuration and execute arbitrary scripts. Patch available at:	Albrecht Guenther PHProjekt 'setup.php' File Upload	High	Secunia Advisory, SA13355, December 2, 2004 Gentoo Linux Security

4.2	http://phprojekt.com/files/4.2/setup.zip Gentoo: http://security.gentoo.org/glsa/glsa-200412-06.xml **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE/** Currently we are not aware of any exploits for this vulnerability.			Advisory, GLSA 200412-06, December 10, 2004 **SUSE Security Summary Report, SUSE-SR:2004:004, December 16, 2004**
Arash Moslehi iWebNegar	An input validation vulnerability exists due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Arash Moslehi IWebNegar Input Validation	High	SecurityFocus, December 15, 2004
Asante FM2008 Managed Ethernet Switch v01.06	A vulnerability exists because the switch has an undocumented default superuser account with a default password, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required.	Asante FM2008 Managed Ethernet Switch Default Backdoor	High	Secunia Advisory,: SA13494, December 16, 2004
Byungchan Kim JSBoard 2.0.7, 2.0.8, JSBoard-win32 1.3.11	A vulnerability exists because the 'include/parse.php' script does not restrict the use of multiple file extensions on uploaded files, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://kldp.net/frs/download.php/1668/jsboard-1.3.13.tar.gz There is no exploit code required; however, a Proof of Concept exploit has been published.	Byungchan Kim JSBoard 'parse.php' Arbitrary Code Execution	High	STG Security Advisory, SSA-20041215-17, December 15, 2004
Cisco Systems Anomaly Detector 3.0 8, Guard 3.0 8.12, 3.0 8	A vulnerability exists because the software contains a default password for an administrative account that is set, without any user's intervention, during installation, which could let a remote malicious user obtain administrative access with superuser privileges. Workaround and upgrade procedures are described in the vendor's advisory, available at: http://www.cisco.com/warp/public/707/cisco-sa-20041215-guard.shtml There is no exploit code required.	Cisco Guard & Traffic Anomaly Detector Default Backdoor	High	Cisco Security Advisory, 63569, December 15, 2004
Cisco Systems Unity Server 2.0-2.4, 2.46, 3.0-3.3, 4.0	A vulnerability exists because several default username/password combinations are present in all available releases of Cisco Unity when integrated with Microsoft Exchange, which could let a remote malicious user obtain unauthorized administrative access. Workaround information available at: http://www.cisco.com/en/US/products/products_security_advisory09186a008037cd59.shtml There is no exploit code required.	Cisco Unity With Exchange Default User Accounts and Passwords	High	Cisco Security Advisory, 63568, December 15, 2004
Ikonboard.com Ikonboard 3.0 .1, 3.1.1, 3.1.2 a	A vulnerability exists in the 'ikonboard.cgi' script due to insufficient validation of user-supplied input in the 'st' and 'keywords' parameters, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Ikonboard 'st' & 'keywords' Input Validation	Medium	SecurityTracker Alert ID, 1012598, December 16, 2004
Kayako Web Solutions eSupport 2.1.2, 2.1.8, 2.2, 2.2.5, 2.3	Multiple input validation vulnerabilities exist: a Cross-Site Scripting vulnerability exists in 'index.php' due to insufficient sanitization of the 'searchm' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in 'index.php' due to insufficient sanitization of the '_i,' 'ticketkey22,' and 'email22' parameters and the email field in the 'Forgot Key' feature, which could let a remote malicious user inject arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published for the Cross-Site Scripting vulnerably.	Kayako ESupport Multiple Cross-Site Scripting and SQL Injection	High	GulfTech Security Research Team Security Advisory, December 19, 2004
Macromedia JRun 3.0, 3.1, 4.0; **Hitachi Cosminexus Enterprise Enterprise Edition 01-02 (*2), 01-01 (*1), Enterprise Standard Edition 01-02 (*2), 01-01**	Multiple vulnerabilities exist: a vulnerability exists due to an implementation error in the generation and handling of JSESSIONIDs, which could let a remote malicious user hijack an authenticated user's session; a Cross-Site Scripting vulnerability exists in the JRUN Management Console, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to an URL parsing error, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists in the verbose logging module. Patches available at: http://www.macromedia.com/support/jrun/updaters.html	Macromedia JRun Multiple Remote Vulnerabilities CVE Name: CAN-2004-0646	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained;	Macromedia Security Bulletin, MPSB04-08, September 23, 2004 US-CERT Vulnerability Notes VU#977440, VU#584958, & VU#668206, October 12, 2004, VU#990200, October 14, 2004 **Hitachi Software**

(*1), Server Web Edition 01-02 (*2), 01-01 (*1)	**Hitachi:** **http://www.hitachi-support.com/security_e/vuls_e/HS04-008_e/01-e.html** We are not aware of any exploits for these vulnerabilities.		and High if arbitrary code can be executed)	**Vulnerability Information, HS04-008, December 16, 2004**
Mantis Mantis 0.9, 0.9.1, 0.10-0.10.2, 0.11, 0.11.1, 0.12, 0.13, 0.13.1, 0.14-14.8, 0.15-0.15.12, 0.16 .0, 0.16-0.16.1, 0.17.0, 0.17-0.17.5, 0.18 a1, 0.18 0rc1, 0.18 0a2-0a4, 0.18, 0.18.2	An unspecified SQL injection vulnerability exists due to a failure to properly sanitize user-supplied input, which could let a remote malicious user compromise the application, obtain sensitive information, modify data, or exploit vulnerabilities in the underlying database implementation. Upgrades available at: http://prdownloads.sourceforge.net/mantisbt/mantis-0.19.1.tar.gz?download Currently we are not aware of any exploits for this vulnerability.	Mantis Unspecified SQL Injection	Medium	SecurityFocus, December 16, 2004
Meik Sievertsen Opentools Attachment Mod 2.3.4-2.3.10	Multiple vulnerabilities exist: a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; and a vulnerability exists due to insufficient handling of 'mod_mime' on several unspecified extensions, which could let a remote malicious user upload arbitrary script files. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=66311 Currently we are not aware of any exploits for these vulnerabilities.	Opentools Attachment Mod Multiple Remote Vulnerabilities	Medium	CastleCops(SM) Security Advisory, December 14, 2004
Michael Kohn asp2php 0.76.23	Two buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists due to boundary errors in the 'preparse()' function, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the in the 'gettoken()' function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Exploit scripts have been published.	Michael Kohn ASP2PHP Remote Buffer Overflows	High	Secunia Advisory, SA13526, December 17, 2004
mnoGoSearch mnoGoSearch 3.1.19, 3.1.20, 3.2.10, 3.2.13-3.2.26	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of input passed to the search results page and the extended/simple search form links, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.mnogosearch.org/Download/mnogosearch-3.2.27.tar.gz There is no exploit code required.	mnoGoSearch Multiple Cross-Site Scripting CVE Name: CAN-2004-1059	High	Secunia Advisory, SA13432, December 13, 2004
moinmoin.wikiwikiweb.de MoniWiki 1.0.8, 1.0.9 .1, 1.0.9	A vulnerability exists in 'UploadFile.php' because the use of multiple file extensions on uploaded files is not restricted, which could let a remote malicious user execute arbitrary code. Update available at: http://kldp.net/forum/forum.php?forum_id=2085 There is no exploit code required.	MoniWiki 'UploadFile.php' Arbitrary Code Execution	High	STG Security Advisory, SSA-20041215-15, December 15,2004
Monolith Productions Contract Jack 1.1, No One Lives Forever 1.0 .004, 2 1.3, Tron 2.0 1.0, 2.0 1.42	A remote Denial of Service vulnerability exists due to a failure to handle exceptional conditions. No workaround or patch available at time of publishing. An exploit script has been published.	Monolith Lithtech Game Engine Remote Denial of Service	Low	Bugtraq, December 13, 2004

Mozilla.org Mozilla Firefox 0.9.2 and Mozilla 1.7.1 on Windows Mozilla Firefox 0.9.2 on Linux	A spoofing vulnerability exists that could allow malicious sites to abuse SSL certificates of other sites. An attacker could make the browser load a valid certificate from a trusted website by using a specially crafted 'onunload' event. The problem is that Mozilla loads the certificate from a trusted website and shows the 'secure padlock' while actually displaying the content of the malicious website. The URL shown in the address bar correctly reads that of the malicious website. An additional cause has been noted due to Mozilla not restricting websites from including arbitrary, remote XUL (XML User Interface Language) files. Workaround: Do not follow links from untrusted websites and verify the correct URL in the address bar with the one in the SSL certificate. SuSE: ftp://ftp.suse.com/pub/suse/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora Legacy: http://download.fedoralegacy.org/redhat/ A Proof of Concept exploit has been published.	Mozilla / Mozilla Firefox 'onunload' SSL Certificate Spoofing CVE Name: CAN-2004-0763	Medium	Cipher.org, July 25, 2004 Secunia, SA12160, July 26, 2004; SA12180, July 30, 2004 SUSE Security Announcement, SUSE-SA:2004:036, October 6, 2004 Conectiva Linux Security Announcement, CLA-2004:877, October 22, 2004 Fedora Legacy Update Advisory, FLSA:2089, October 27, 2004 **US-CERT Vulnerability Note, VU#262350, December 17, 2004**
Multiple Vendors CVSTrac 1.1-1.1.4; OpenPKG Current, 2.1, 2.2	A Cross-Site Scripting vulnerability exists due to a insufficient sanitization of user-supplied URI data prior to including it in dynamically generated web page content, which could let a remote malicious user execute arbitrary HTML and script code. CVSTrac: http://www.cvstrac.org/cvstrac-src-1.1.5.tar.gz OpenPKG: ftp://ftp.openpkg.org/release/ There is no exploit code required.	CVSTrac Unspecified Cross-Site Scripting CVE Name: CAN-2004-1146	High	OpenPKG Security Advisory, OpenPKG-SA-2004.056, December 17, 2004
Multiple Vendors Debian Linux 3.0 spar, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.7	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the DICOM dissector; a remote Denial of Service vulnerability exists in the handling of RTP timestamps; a remote Denial of Service vulnerability exists in the HTTP dissector; and a remote Denial of Service vulnerability exists in the SMB dissector when a malicious user submits specially crafted SMB packets. Potentially these vulnerabilities may also allow the execution of arbitrary code. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200412-15.xml Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Multiple Denial of Service & Potential Code Execution Vulnerabilities CVE Names: CAN-2004-1139 CAN-2004-1140 CAN-2004-1141 CAN-2004-1142	Low/High (High if arbitrary code can be executed)	Ethereal Security Advisory, enpa-sa-00016, December 15, 2004
PHP Group PHP 4.3.6-4.3.9, 5.0 candidate 1-canidate 3, 5.0 .0-5.0.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'pack()' function, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the 'unpack()' function, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'safe_mode' when executing commands, which could let a remote malicious user bypass the security restrictions; a vulnerability exists in 'safe_mode' combined with certain implementations of 'realpath(),' which could let a remote malicious user bypass security restrictions; a vulnerability exists in 'realpath()' because filenames are truncated; a vulnerability exists in the 'unserialize()' function, which could let a remote malicious user obtain sensitive information or execute arbitrary code; a vulnerability exists in the 'shmop_write()' function, which may result in an attempt to write to an out-of-bounds memory location; a vulnerability exists in the 'addslashes()' function because '\0' ir not escaped correctly; a vulnerability exists in the 'exif_read_data()' function when a long sectionname is used, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in 'magic_quotes_gpc,' which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.php.net/downloads.php Mandrake: http://www.mandrakesecure.net/en/ftp.php There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHP Multiple Remote Vulnerabilities CVE Names: CAN-2004-1018 CAN-2004-1063 CAN-2004-1064 CAN-2004-1019 CAN-2004-1020 CAN-2004-1065	Medium/ High (High if arbitrary code can be executed)	Bugtraq, December 16, 2004
phpBB Group phpBB 2.0.7 a, 2.0.7	A vulnerability exists due to failure to properly sanitize user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.phpbb.com/downloads.php There is no exploit code required.	PHPBB IMG Tag HTML Injection	High	SecurityFocus, December 17, 2004

phpBB Group phpBB 2.0.0-2.0.9	Multiple vulnerabilities exist: a vulnerability exists in 'viewtopic.php' due to insufficient sanitization of the 'highlight' parameter, which could let a malicious user obtain sensitive information or execute arbitrary code; a vulnerability exists due to insufficient sanitization of input passed to the username handling, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists due to insufficient sanitization of input passed to the username handling before being used in an SQL query, which could let a malicious user execute arbitrary code. **According to reports, this vulnerability is being actively exploited by the Santy.A worm. The worm appears to propogate by searching for the keyword 'viewtopic.php' in order to find vulnerable sites.** Upgrades available at: http://www.phpbb.com/downloads.php There is no exploit code required; however, a Proof of Concept exploit script has been published. **Vulnerability has appeared in the Press and other public media.**	PHPBB Login Form Multiple Input Validation	High	SECUNIA ADVISORY ID: SA13239, November 19, 2004 **US-CERT Technical Cyber Security Alert, TA04-356A, December 21, 2004** **US-CERT Vulnerability Note, VU#497400, December 21, 2004**
phpformmail.sourceforge.net PHPFormMail prior to 1.07.0	A Cross-Site Scripting vulnerability exists in the 'output_html()' function in 'formmail.php' and another unspecified parameter due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://www.boaddrink.com/projects/phpformmail/download.php Currently we are not aware of any exploits for this vulnerability.	PHPFormMail Cross-Site Scripting	High	Secunia Advisory, SA13576, December 20, 2004
PhpGedView PhpGedView 2.52.3, 2.60, 2.61, 2.61.1, 2.65 beta5	A Cross-Site Scripting vulnerability exists in 'source.php,' Imageview.PHP,' 'Login.PHP,' 'Gedrecord.PHP,' 'Gdbi_interface.PHP,' 'Relationship.PHP,' 'Calendar.PHP,' 'Timeline.PHP,' and 'Placelist.PHHP' due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/phpgedview/phpGedView-2.65.2.zip?download There is not exploit required; however, Proofs of Concept exploits have been published.	PhpGedView Source.PHP Cross-Site Scripting CVE Name: CAN-2004-0067	High	SecurityFocus, December 13, 2004
Ricoh Aficio 450 PCL Printer, 455 PCL Printer	A remote Denial of Service vulnerability exists due to an error in the handling of ICMP packets. No workaround or patch available at time of publishing. An exploit script has been published.	Ricoh Aficio 450/455 PCL Printer Remote ICMP Denial of Service	Low	Secunia Advisory, SA13475, December 17, 2004
Singapore singapore 0.9 a beta, 0.9 beta, 0.9.1 beta-0.9.10 beta, 0.9.10	Multiple vulnerabilities exist: a vulnerability exists in 'thumb.php' due to insufficient validation of the 'showThumb()' function, which could let a remote malicious user download arbitrary files; a vulnerability exists in 'admin.class.php' in the 'addImage()' function, which could let a remote malicious user upload files containing PHP code; a Directory Traversal vulnerability exists in 'admin.class.php' which could let a remote malicious user delete arbitrary directories; and multiple unspecified Cross-Site Scripting vulnerabilities exist which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/singapore/singapore-0.9.11.zip?download There is no exploit code required.	Singapore Image Gallery Multiple Remote Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	SIG^2 Vulnerability Research Advisory, December 16, 2004
SIR GNUBoard 3.30-3.39	A vulnerability exists in 'index.php' due to insufficient verification of the 'doc' parameter before being used to include files, which could let a remote malicious user execute arbitrary code. Update available at: http://sir.co.kr/?doc=bbs/gnuboard.php&bo_table=pds&page=1&wr_id=1871 There is no exploit code required.	GNUBoard 'doc' Parameter Arbitrary File Inclusion	High	STG Security Advisory, SSA-20041214-14, December 15,2004
Symantec Brightmail Anti-Spam 6.0.1	Two vulnerabilities exist: a remote Denial of Service vulnerability exists because the Sieve module fails to recognize malformed RFC 822 MIME attachment boundaries; and a remote Denial of Service vulnerability exists because Spamhunter fails to convert certain valid character encoding sets to UTF. Patch available at: ftp://ftp.symantec.com/public/english_us_canada/products/sba/sba_60x/updates/Patch134.zip Currently we are not aware of any exploits for these vulnerabilities.	Symantec Brightmail Remote Denials of Service	Low	SecurityTracker Alert ID, 1012612, December 17, 2004
Ueli Weiss IMG2ASCII 1.15, 1.16	A vulnerability exists in the 'ascii.php' script because the use of multiple file extensions on uploaded files is not restricted, which could let a remote malicious user execute arbitrary code. Upgrades available at:	Ueli Weiss IMG2ASCII Unauthorized File Upload	High	SecurityTracker Alert ID, 1012622, December 19, 2004

	http://sourceforge.net/project/showfiles.php?group_id=85061&package_id=87928 There is no exploit script required.			
wordpress.org WordPress 1.2, 1.2.1	Various Cross-Site Scripting vulnerabilities exists due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://wordpress.org/latest.tar.gz There is not exploit code required; however, Proofs of Concept exploits have been published.	Wordpress Multiple Cross-Site Scripting	High	SecurityFocus, December 16, 2004
WorkBoard WorkBoard 1.2	Multiple Cross-Site Scripting vulnerabilities exists due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code. This application is not supported by the vendor. There is no exploit code required; however, Proofs of Concept exploits have been published.	WorkBoard Multiple Cross-Site Scripting	High	SecurityFocus, December 17, 2004

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
December 19, 2004	ethereal-0.10.8.tar.gz	N/A	Ethereal is a GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
December 18, 2004	68-1.grx.zip 68-2.grx.zip	No	Exploit for the Anoakie Turner GREED 'DownloadLoop()' Function vulnerability.
December 18, 2004	71-1.cal.zip 71-2.cal.zip	Yes	A Proof of Concept exploit for the Andrew W. Rogers pcal Buffer Overflow vulnerabilities.
December 17, 2004	29-1.asp.zip 29-2.asp.zip	No	Exploit for the ASP2PHP Remote Buffer Overflow vulnerabilities.
December 17, 2004	31.emelody.zip	No	Exploit for the Michael Kohn Ringtone Tools parse_emelody() Buffer Overflow vulnerability.
December 17, 2004	34.frm.zip	No	Exploit for the Michael Kohn Visual Basic to C/GTK (vb2c) gettoken() Buffer Overflow vulnerability.
December 17, 2004	35.abc.zip	Yes	A Proof of Concept exploit for the Jean-François Moine abcm2ps put_words() Buffer Overflow vulnerability.
December 17, 2004	36-1.abc.zip	No	A Proof of Concept exploit for the aChristoph Dalitz abctab2ps Buffer Overflows.
December 17, 2004	36-2.abc.zip	No	A Proof of Concept exploit for the bctab2ps Trim_Title Function ABC File Remote Buffer Overflow vulnerability.
December 17, 2004	38-1.abc.zip 38-2.abc.zip	No	Exploits for the ABC2MIDI Multiple Stack Buffer Overflow vulnerability.
December 17, 2004	45.pgn.zip	No	A Proof of Concept exploit for the GNU pgn2web process_moves() Buffer Overflow vulnerability.
December 17, 2004	46.mesh.zip	No	A Proof of Concept exploit for the Helmut Cantzler Mesh Viewer dxfin() Buffer Overflow vulnerability.
December 17, 2004	53.csv.zip	Yes	A Proof of Concept exploit for the BSD csv2xml get_csv_token() Buffer Overflow vulnerability.
December 17, 2004	58.xml.zip	No	Script that exploits the o3read parse_html() Buffer Overflow vulnerability.
December 17, 2004	61.html.zip	No	A Proof of Concept exploit script for the html2hdml remove_quote() Buffer Overflow vulnerability.
December 17, 2004	74.abc.zip	No	A Proof of Concept exploit for the GNU jcabc2ps switch_voice() Buffer Overflow vulnerability.
December 17, 2004	79.abc.zip	No	Exploit for the Chris Walshaw abc2mtex process_abc() Buffer Overflow vulnerability.
December 17, 2004	80.abc.zip	No	Exploit for the Guido Gonzato abcpp handle_directive() Buffer Overflow vulnerability.
December 17, 2004	81.rtf.zip	No	A Proof of Concept exploit for the GNU UnRTF Font Table Conversion Buffer Overflow vulnerability.
December 17, 2004	winRAR3_40BufferOverflowPOC.c	No	Exploit for the RARLAB WinRAR File Name Remote Client-Side Buffer Overflow vulnerability.

December 16, 2004	1.xls.zip	No	Exploit for the David Giffin xlreader book_format_sql() Buffer Overflow vulnerability.
December 16, 2004	10.list.zip	No	Exploit for the GNU jpegtoavi get_file_list_stdin() Buffer Overflow vulnerability.
December 16, 2004	11.mail.zip	Yes	Script that exploits the Bolthole Filter save_embedded _address() Buffer Overflow vulnerability.
December 16, 2004	12.html.zip	No	Script that exploits the Patric Müller Vilistextum get_attr() Buffer Overflow vulnerability.
December 16, 2004	13.txt.zip	Yes	Exploit for the AtBas 2fax expandtabs() Buffer Overflow vulnerability.
December 16, 2004	2.dxf	No	A Proof of Concept exploit for the GNU DXFscope dxfin() Buffer Overflow vulnerability.
December 16, 2004	20.avi	Yes	Exploit for the GPL Xine open_aiff_file() Buffer Overflow vulnerability.
December 16, 2004	22.S.zip	Yes	Exploit for the LGPL NASM error() Buffer Overflow vulnerability.
December 16, 2004	3.msg.zip	No	A Proof of Concept exploit script for the Little Igloo LinPopUp strexpand() Buffer Overflow vulnerability.
December 16, 2004	5.rtf.zip	No	A Proof of Concept exploit script for the GNU rtf2latex2e ReadFontTbl() Buffer Overflow vulnerability.
December 16, 2004	7.3ds.zip	No	A Proof of Concept exploit script for the GNU Convex 3D readObjectChunk() Buffer Overflow vulnerability.
December 16, 2004	9.http.zip	No	Proof of Concept exploit for the Gastón Kleiman Yanf get() Buffer Overflow vulnerability.
December 16, 2004	ability-2.34-ftp-stor.py un-aftp.c	No	Exploits for the Ability Server 'APPE FTP' Command Buffer Overflow vulnerability.
December 16, 2004	firstclass_search_exploit.c secunia.com-advisories-13415.c	Yes	Script that exploits the OpenText FirstClass HTTP Daemon Search Function Remote Denial of Service vulnerability.
December 15, 2004	17-s.c	Yes	Exploit for the GNU MPlayer ASF Streams Processing Buffer Overflow vulnerability.
December 15, 2004	21.hpgl.gz	Yes	Exploit for the GNU CUPS HPGL ParseCommand() Buffer Overflow vulnerability.
December 15, 2004	49.list.zip	No	Exploit for the GNU ChBg simplify_path() Buffer Overflow vulnerability.
December 15, 2004	8.list	No	Exploit for the Michael Hipp mpg123 find_next_file() Buffer Overflow vulnerability.
December 15, 2004	napshare_srv.c napshare_srv_2.c	No	Scripts that exploit the GNU NapShare auto_filter_extern() Buffer Overflow vulnerability.
December 15, 2004	phpbb2memorydump.zip	Yes	Exploit for the PHP Multiple Local And Remote Vulnerabilities.
December 15, 2004	rpcl_icmpdos.c	No	Script that exploits the Ricoh Aficio 450/455 PCL Printer Remote ICMP Denial of Service vulnerability.
December 14, 2004	scm_send_dos.c	Yes	Script that exploits the Multiple Vendors Linux Kernel Auxiliary Message Layer State Error vulnerability.
December 13, 2004	ceaglesock.zip	No	Exploit for the Codename Eagle UDP Packet Processing Remote Denial of Service vulnerability.
December 13, 2004	igmp.c	Yes	Exploit for the Multiple Vendors Linux Kernel IGMP Integer Underflow Vulnerabilities.
December 13, 2004	lithsock.zip	No	Exploit for the Monolith Lithtech Game Engine Remote Denial of Service vulnerability.

[back to top]

Trends

- The US-CERT continues to receive reports of increased phishing activity during this holiday season. Online shoppers are urged to take special caution while conducting on-line transactions via the Internet. For additional information regarding phishing and social engineering, please visit the following links:
  - http://www.us-cert.gov/cas/tips/ST04-014.html
  - http://www.ftc.gov/bcp/conline/pubs/alerts/shopalrt.htm
  - http://www.ftc.gov/bcp/conline/edcams/onlineshopping/coninfo.html
  - http://www.fbi.gov/pressrel/pressrel04/idtheft111704.htm

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Sober-I	Win32 Worm	Increase	November 2004
3	Zafi-B	Win32 Worm	Stable	June 2004
4	Netsky-D	Win32 Worm	Decrease	March 2004
5	Netsky-Z	Win32 Worm	Stable	April 2004
6	Netsky-Q	Win32 Worm	Stable	March 2004
7	Bagle-AA	Win32 Worm	Stable	April 2004
8	Bagle-AT	Win32 Worm	Stable	October 2004
9	Bagle-AU	Win32 Worm	Stable	October 2004
10	Netsky-B	Win32 Worm	Stable	February 2004

Table Updated December 21, 2004

Viruses or Trojans Considered to be a High Level of Threat

- **Viruses or Trojans Considered to be a High Level of Threat**

  - F-Secure has released their 'F-Secure Corporation's Data Security Summary for 2004.' New trends in 2004 were primarily the massive increase in phishing email scams, and the introduction of open-source botnets - networks of infected machines harnessed for malicious operations, and for-profit virus-writing. For more information, see: http://www.f-secure.com/2004/
  - Sanity.A: A Web worm that identifies potential victims by searching Google is spreading among online bulletin boards using a vulnerable version of the program phpBB. Almost 40,000 sites may have already been infected. Using Microsoft's Search engine to scan for the phrase 'NeverEverNoSanity'--part of the defacement text that the Santy worm uses to replace files on infected Web sites--returns nearly 39,000 hits. For more information, see: http://news.com.com/Net%2Bworm%2Busing%2BGoogle%2Bto%2Bspread/2100%2D7349_3%2D5499725.html.

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Lateda		Trojan
Backdoor.Masteseq		Trojan
Backdoor.Subot		Trojan
Backdoor.Tabdim		Trojan
Backdoor.Win32.Jix.a	Exploit-MS04-011.gen W32.Janx WORM_JANZ.A Worm/Zusha.A NewHeur_PE	Trojan
Cabir.F	SymbOS/Cabir.F EPOC/Cabir.F Worm.Symbian.Cabir.F Tee222 virus	Internet Worm
Cabir.G	SymbOS/Cabir.G EPOC/Cabir.G Worm.Symbian.Cabir.G SEXXXY virus	Internet Worm
Downloader-TA		Trojan
Email-Worm.Win32.Breacuk.a	W32/Beaker-A Worm/Breacuk.A I-Worm/Breacuk.A Win32.Beaker.A@mm NewHeur_PE	Win32 Worm
MGDropper	SymbOS/MGDropper Metal Gear trojan	Trojan
Troj/Bancban-AN	Trojan-Spy.Win32.Banbra.ad PWS-Bancban.gen.b	Trojan
Trojan.Netdepix	W32.Netdepix	Trojan
Trojan.PSW.LdPinch.ht	Trojan-PSW.Win32.LdPinch.ht Backdoor.Damrai.A Damrai.A	Trojan
VBS.Feadfe@mm		Visual Basic Script Worm
VBS.Sorpe.A@mm	Trojan.VBS.Spore.a VBS.Sorpe.B@mm VBS/Sorpe@MM	Visual Basic Script Worm
W32.Envid.B@mm		Win32 Worm

W32.Looked	Virus.Win32.Delf.62976 W32/HLLP.Philis.j	Win32 Worm
W32.Mugly.C@mm	Email-orm.Win32.Wurmark.b W32/Wurmark-C WORM_MUGLY.C	Win32 Worm
W32.Pulkfer		Win32 Virus
W32/Atak-I	Email-Worm.Win32.Atak.i Worm.Mydoom.Gen-unp W32/Atak.i@MM Worm/Atak.M W32/Atak.j@MM Email-Worm.Win32.Atak.h Win32.HLLM.Atak W32/Atak-J WORM_ATAK.I Worm/Atak.I W32/Atak.I@mm I-Worm/Atak.I Win32.Atak.I@mm Worm.Mydoom.Gen-unp W32/Mydoom.gen.worm NewHeur_PE	Win32 Worm
W32/Delf-JB		Win32 Virus
W32/Forbot-BI	WORM_WOOTBOT.AQ	Win32 Worm
W32/Forbot-CY		Win32 Worm
W32/Forbot-DA	Backdoor.Win32.Wootbot.ab W32/Gaobot.worm.gen	Win32 Worm
W32/Forbot-EQ		Win32 Worm
W32/Oddbob-A		Win32 Worm
W32/Protoride-Z		Win32 Worm
W32/Rbot-RR		Win32 Worm
W32/Rbot-RW		Win32 Worm
W32/Rbot-RY		Win32 Worm
W32/Rbot-SB	W32/Sdbot.worm.gen.j	Win32 Worm
W32/Sdbot-SI	W32/Sdbot.worm.gen Backdoor.Win32.SdBot.gen	Win32 Worm
W32/Wort-D		Win32 Worm
W97M.Banedi		Word 97 Macro Virus
W97M.Grurev		Word 97 Macro Virus
Win32.Holax.A	HTML.Holax.A Win32/Holax.Trojan	Win32 Virus
Win32.Kol.F	BackDoor-CGP Win32/PWS.Xuxx.Trojan Keylogger.Trojan Win32/Zins.B Backdoor.Zins.gen	Trojan
Win32.Kol.G	BackDoor-AWV W32/Banker.CM BKDR_HACDEF.K Win32/Kol.F.Trojan Backdoor.Trojan Backdoor.Win32.Zins.gen Win32/Zins.C Troj/Zins-A	Trojan
Win32.Muquest.A	W32/Delf.ED Win32/Requester.5.Proxy.Trojan TrojanProxy.Win32.Delf.h	Trojan
Win32.Plimp.A	BackDoor-CIG W32.IRCBot Win32/IRCBot.23552.Trojan W32/SDBot.AXV W32/SillyTrojan.P@bd Win32/Small.BL BKDR_SMALL.BL Troj/Small-BC Backdoor.Win32.Small.bl	Trojan
Worm.Win32.Drew.a	xploit-DcomRpc.g.gen Win32.HLLW.Drew W32/Drew.A Win32:RPCexploit Exploit.DCOM.Gen W32/Drew.A.worm Wwin32/Drew.A	Win32 Worm

WORM_SANTY.A	Perl.Santy Santy Net-Worm.Perl.Santy.a PHP/Santy.worm t-Worm.Perl.Santy.a	Win32 Worm
X97M.Frost		Excel 97 Macro Virus

[back to top]

Last updated December 22, 2004